Cranfield University

Dhanapala Jayakody-Arachchige

Bayesian Model
for Strategic Level Risk Assessment in
Continuing Airworthiness of Air Transport

School of Engineering

PhD

Cranfield University

School of Engineering

PhD

Dhanapala Jayakody-Arachchige

Bayesian Model for Strategic Level Risk Assessment in Continuing Airworthiness of Air Transport

Supervisors: Dr Simon Place/ Mr John Snow

Academic Year 2007 to 2010

This thesis is submitted in partial fulfilment of the requirement
for the Degree of Doctor of Philosophy

‘Be sensitive to risk. use a net always’, said the spider.

“Knowledge is limiting. To learn new things, one must escape from what was learnt and carefully observe the state of nature around”.
(Jiddu Krishnamoorthy)

Abstract

Continuing airworthiness (CAW) of aircraft is an essential pre-requisite for the safe operation of air transport. Human errors that occur in CAW organizations and processes could undermine the airworthiness and constitute a risk to flight safety. This thesis reports on a generic Bayesian model that has been designed to assess and quantify this risk.

The model removes the vagueness inherent in the subjective methods of assessment of risk and its qualitative expression. Instead, relying on a transparent, structured mathematical process based on Bayes' Theorem of conditional probabilities, the model yields a quantitative risk output expressed as a probability of error coupled with a probability of consequence based on data.

The Bayesian model has 184 nodes and 1138 parameters that define causal factors for error against which data is collected as either beliefs or evidence, the latter returning more reliable results. Beliefs could be gradually replaced with evidence as they become available, improving fidelity. The generic model can be modified by adding or truncating parameters to suit conditions applicable to specific organizations or similar groups.

The model was validated using field data from a cargo operator using large western jet freighters, covering 34,338 sectors of which 193 carried human error. Separate tests were performed simulating the operator's belief that it was operating to global standards.

The output for belief was consistent with global and UK flat rate safety levels, achievable if the operator flew 3M and 6M sectors respectively according to their belief. However, the output from evidence returned a risk level more severe than the belief, partly driven by the allowance for unknowns built into the computing technique and part by the relatively small number of sectors considered. In "what-if" prediction mode the model calculates the change in risk level due to new errors, and through sensitivity analysis it can identify and rank performance indicators.

In CAW organizations subjected to Risk Based Oversight (RBO) concept and ICAO mandate on Safety Management System (SMS), the model can set risk threshold levels for individual organizations, to measure variations, and by continuous updating, to monitor safety performance at strategic level. Sharing data and with agreed performance levels, the Regulator and operators should be able negotiate an oversight plan. Using the model pro-actively, the organization could exercise a degree of self-regulation, thereby accruing cost benefits through reduced Regulator oversights.

Acknowledgements

First of all I must express my thanks to David Lewis (former Deputy Chief Surveyor, UK CAA) Dave Howson (UK CAA) and my supervisor Dr Simon Place, for entrusting me to undertake this research study under a joint EPSRC-UK CAA industrial CASE Award. I am very grateful to them and to the organizations they represented.

With gratitude I acknowledge the generous financial assistance given by The International Air Cargo Association through its Walter H Johnson Jr PhD Scholarship 2008, enabling me to extend the scope of research to cargo aircraft. My sincere thanks go to the Officers and members of TIACA, to its Educational Committee, and especially to Beverly Weinsier who kindly coordinated all the formalities.

At UK CAA, credit is due to Adrian Sayers, Ben Alcott, Barrie Pilcher, Dave Marsh, Dave Wright, Graham Rourke, Graham Wheeler, Hazel Courteney, Jim McKenna, Peter Noad, Ray Nimmo and Tom Hamilton for facilitating my work through their good offices. I thank all other departmental heads and staff who provided information and assisted the project in other ways, and members of Safety Analysis and Research, for their close support to my work during my short tenure there.

Without specific industry participants, whom I am not at liberty to name, this study would have been an inanimate academic exercise. You put the breath into it, providing field data, assisting and encouraging the study. I admire your courage to serve the industry with a true spirit of commitment to flight safety. However, I can mention Jim Jones and Chris Clark of UK FSC, Mick Skinner of CHIRP, John Saul IFA and FSF, representing industry's flight safety interests and ALAE representing licensed engineers.

Your support has been a great strength to this study, and I hope that both UK CAA and industry will benefit from this work in return. Thank you.

At Cranfield, I owe my thanks to Professor Braithwaite, Head of Air Transport Department, and to Barbara and her staff for their indispensable admin support to the project, to Dr Adam Zagorecki of DCMT Shrivenham (former Genie & Smile team member, University of Pittsburg) for tutoring me on finer points of BBN design, and to Dr Simon Place and Mr John Snow for supervising my work. Simon and John, thank you for being caring and ever so polite mentors and guides, the best that anyone could get.

I thank all my peers, well wishers, friends and relatives, who supported and encouraged me during this long assignment. A really special thank you is reserved to my beloved wife, Merican, for the loving care and support she gave me, for her patience and forbearance that finally helped me to conclude this research study successfully.

Thank you all.

Dedicated

to

my Parents

'whose wisdom set me on a quest for knowledge'

Acronyms

AAIB	Aviation Accident Investigation Board
AC	Aircraft (or Air Conditioning) (or Alternating Current)
ADD	Acceptable Deferred Defect
ADREP	Accident (or Incident) Data Reporting
AGL	Above Ground Level
AHP	Analytical Hierarchical process
ALAE	Association of Licensed Aircraft Engineers
ALARP	As Low As Reasonably Practicable
AM	Accountable Manager
AMM	Aircraft Maintenance Manual
AMMP	Aviation Maintenance Monitoring process
AMO	Approved Maintenance organization
AMP	Aircraft Maintenance Program (or Plan)
ANO	Air Navigation Order
AO	Approved Organization
AOC	Air Operator Certificate
AOR	Air Occurrence Report
APU	Auxiliary Power Unit
AQD	Business entity named AQD Superstructure
ARC	Airworthiness Review Certificate
ASRM	Aviation Safety Risk Model
ASRM	Aviation System Risk Model
ATC	Air Traffic Control
ATC	Air Traffic Control
ATO	Approved Training Organization
ATS	Air Traffic Services
AUW	All-up Weight
AWOPS	All Weather Operations
BA	British Airways
BBN	Bayesian Belief Network
BCAR	British Civil Aviation Regulations
BTA	Bow Tie Analysis
CAA	Civil Aviation Authority
CAME	Continuing Airworthiness Management exposition
CAMO	Continuing Airworthiness Management organization
CAP	Civil Air Publication
CAS	Codex Alimentarius Commission (Food Standards Commission)
CASE	Collaborative Awards in Science and Engineering

CAW	Continuing Airworthiness
CB	Contact Breaker
CBT	Computer Based Training
CCA	Common Cause Analysis
CEO	Chief Executive Officer
CF	Carried forward
CFIT	Controlled Flight into Terrain
CHIRP	Confidential Human Factors Incident Reporting Programme
CIAIAC	Commission for the Investigation of Civil Aviation Incidents
CIS	Confederation of Independent States (Former Soviet Union)
CPT	Conditional Probability Table
CRS	Certificate of Release to service
CWT	Centre Wing tank
DA	Design Authority
DAG	Directed Acyclic Graph
DECU	Digital Engine Control Unit
DETR	Department of the Environment, Transport and the Regions
DfT	Department for Transport
DOA	Design Organization Approved
DV	Deterministic Variable
EASA	European Aviation Safety Agency
EC	European Council
ECCAIRS	European Co-ordination Centre for Aircraft Incident Reporting System
ECI	Error Criticality Index
ECOSOC	Economic and Social Council
EGPWS	Enhanced Ground Proximity Warning System
ELEV PCU	Elevator Power Control Unit
EMOS	Type of digital information service
EPR	Engine Pressure ratio
EPSRC	Engineering and Physical Sciences Research Council
ES	Expert System
ETA	Event Tree Analysis
ETOPS	Extended-range Twin-engine Operational Performance Standards
EU	European Union
EXCEL	Microsoft Excel Program
FAA	Federal Aviation Administration
FAO	Food and Agriculture Organization
FEMA	Failure Effects and Modes Analysis
FL	Fuzzy logic
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis

FOD	Foreign Object Damage
FOHE	Fuel Oil Heat Exchanger
FORAS	Flight Operations Risk Analysis System
FSC	Flight Safety Committee
FSS	Flight Standards Service
FTA	Fault Tree Analysis
GDP	Gross Domestic Products
GENIE	Name of a BBN software program – Genie & Smile
GOR	Ground Occurrence Report
GPU	Ground Power Unit
GSE	Ground Support Equipment
HAZOPS	Hazard and Operability Studies
HF	Human Factors
HFACS	Human Factors Analysis and Classification System
HFACS(ME)	HFACS (Maintenance Extension)
HILAS	Human Integration into the Lifecycle of Aviation Systems
HM	Her Majesty's
HR	Human Resources
HSE	Health and Safety Executive
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ID	Influence Diagram
ILS	Integrated Logistic Support
IOSA	IATA Operational Safety Audit
ISO	International Organization for Standardization
IT	Information Technology
JAR	Joint Airworthiness Regulations
KPI	Key Performance Indicator
LAE	Licensed Aircraft Engineer
LRU	Line Replacement Unit
MCDA	Multivariate Criteria Decision Analysis
MD	McDonnell Douglas
MEDA	Maintenance Error Decision Aid
MEL	Minimum Equipment List
MEMS	Maintenance Error Management System
MEPM	Maintenance Error Prediction Model
MNPS	Minimum Navigation Performance Specification
MOC	Maintenance Operation centre
MOR	Mandatory Occurrence Report
MRO	Maintenance, Repair and Overhaul Organization
MSG	Maintenance System Guide

NAA	National Aviation Authority
NBC	Nuclear Biological and Chemical
NETICA	Name of a BBN software program
NK	Not Known
NL_CAA	Civil Aviation Authority of the Netherlands
NLR	National Aerospace Laboratory
NORSYS	Business entity of the name NORSYS
NTSB	National Transportation Safety Board
OA	Organization Approved
OEM	Original Equipment Manufacturer
OME	Original Manufacturer's Equipment
PC	Personal Computer
PDS	Post Design services
PH	Philip Hampton
PMA	Parts Manufacturer Approved
POA	Production Organization Approved
PSO	Particle Swarm Optimization
PSZ	Public Safety Zones
QA	Quality Audit
QMS	Quality Management System
RAF	Royal Air Force
RAM	Risk Assessment Model
RBO	Risk Based Oversight
RMS	Root Mean Square
ROWI	Regulatory Oversight Weighting Index
RTB	Return to Base
RV	Random Variable
RVSM	Reduced Vertical Separation minima
SARP	Standards and Recommended Practices
SHEL	Software Hardware Environment Liveware
SI	Structural Integrity
SIWG	Structural Integrity Working group
SMILE	Name of a BBN software program – Genie & Smile
SMM	Safety Management Manual
SMS	Safety Management System
SOI	Statement of Operating Intent
SPAS	Safety Performance Analysis System
SRG	Safety Regulation Group
TC	Type Certificate
TCDS	Type Certificate Data Sheets
TCSEC	Trusted Computer System Evaluation Criteria

TIACA	The International Cargo Association
TO	Take-Off
TO	Training Organization
TQM	Total Quality management
TRAX	Aircraft maintenance management system software
TTE	Tools and Test Equipment
TU	Tupolev
UC	Undercarriage
UK	United Kingdom
UK FSC	United Kingdom Flight Safety Committee
US	United States
UTC	Co-ordinated Universal Time
WHO	World Health organization

Intentionally Blank

Table of Contents

Intentionally Blank

Table of Figures

Intentionally Blank

Table of Tables

Chapter One

Introduction

1.1 Background

1.1.1 Role of human error in accidents

Major aircraft accidents often generate sensational media headlines, creating a perception that air transport has high risk and drawing public attention to shortcomings in flight safety. Quite often human error is cited as a causal factor for some of the accidents. Human error is a well known hazard in any industry and air transport is no exception[1].

Human errors occur in all aspects of aircraft operations, namely, in maintenance and ground handling, in flight operations, in air traffic control and in airfield management. According to an analysis[5] of global air accidents over a period of 50-years, pilot error is by far the largest causal factor (50%) for accidents. At 6% other human errors that include maintenance error, shortfalls in continuing airworthiness (CAW) processes such as engineering and integrated logistic support rank at 5th place. Other research data[6, 7, 8] indicate that between 6 to 15% of all reported incidents in air transport are attributed to maintenance errors. If left uncontrolled, human error would lead to loss of public confidence in air transport and consequential wide ranging economic losses.

1.1.2 Case studies of human error in CAW

This study investigates human error in CAW process in which maintenance and ground handling is one part, and organization and management is the other part. The total loss of Alaskan Airline Flight 261 MD-83 on 31 January 2000[2], the mid-flight loss of a large fuselage panel together with a cabin attendant from Aloha Flight 243 Boeing 737 on 28 April 1988[3], and the serious incident to BA G-YMME, Boeing 777, at Heathrow airport on 10 June 2004[4] were typical accidents due to human error in CAW.

The circumstances leading to the G-YMME incident demonstrate the way simple mistakes get complicated by a chain of events. An unidentified engineer had removed a purge door to ventilate an aircraft fuel tank that was being prepared for an internal structural inspection. The purge door removal was a deviation from the authorized procedures for a Boeing 777 aircraft, yet the engineer had failed to document his action by raising a supplementary job card and an entry on the aircraft log to alert the

task controller, as they were required to do. Thus, the knowledge of the repair status and its control were lost. Few days later, other engineers recovered the aircraft after the tank inspection, unaware that a purge door had been left open. A leak detection test of the tank had been completed but it failed to reveal the open door because the AMM specified fuel level for the test was, mistakenly, lower than the level of the door.

After releasing the aircraft to service from maintenance, it continued to fly for one month on short routes without revealing the open door, until the day when it was scheduled to fly a long route carrying a much larger fuel load. This time, as the aircraft was rotating for take-off and climbing, fuel cascaded out of the tank, trailing a long fuel stream behind it. If a stray spark had ignited the fuel vapor, it could have been fatal to the occupants and to the people on the ground. Fortunately, the aircraft was safely recovered back to Heathrow. Accident investigators identified a number of individual and organizational errors that contributed to this event, as well as errors attributed to the aircraft Design Authority.

Full case studies for the G-YMME incident and four other major accidents are described in Appendix 2 to demonstrate different forms of system failure arising from combinations of unrelated human errors and missed timely intervention.

1.1.3 Organizational and management errors

Errors are not confined to the in-service phase of an aircraft's life cycle. They may occur even during design, manufacture, production of aircraft and the planning and implementation of post production services such as integrated engineering and logistic support. Often, despite design reviews built into equipment development programs, some errors pass undetected and remain dormant in the fabric of the aircraft, in its support equipment, or in documentation relating to the product. Unfortunately they resurface at a later time leading to an accident when other conditions line-up[1]. The loss of Concorde Flight at Paris[9] and the near loss of BA Flight at Heathrow[10] were associated with shortcomings in the design and development of equipment. With in-service experience, the Concorde's design shortcomings had been recognized, yet the Design Authority had failed to act on them, see Appendix 2.

Away from the critical human-machine interface, occasional inadvertent errors are made by managers at all levels of responsibility and authority during decision making process relating to organizational and management functions. Often, the conflict between safety and commercial objectives is the root cause, and they have far reaching consequences. When exposed, quite often they are dressed down as errors

of judgment or even simply swept under the carpet as inconsequential, much to the dismay and derision of work face employees who are affected by management errors. *"Errors of maintenance technicians are the visible manifestation of problems with roots deep in the organization"* according to Hobbs[11] who reports on human factors that lead to accidents.

1.1.4 Role of risk assessment in current industry requirements

Since error occurrence is random in nature and consequences are variable, there ought to be a means of discriminating the outcome of an error that could occur in the system in a meaningful way. The concept of "risk" evolves from this need and the need for public services such as air transport to be regulated in order to minimize the risk. The UK Air Navigation Order (ANO)[12] legally empowers the UK Civil Aviation Authority (CAA) to oversee that all approved organizations responsible for the delivery of a safe flight comply with appropriate safety regulations, and to assess the risk according to the way they conduct their operations.

Hitherto, risk assessment has been based on expert opinion and judgement, on a criterion that has been expressed qualitatively and whose rationale remained within the knowledge of the subject expert. In a modern business environment of competing priorities and wide range of stakeholder interests, existing risk assessment techniques are challenged by other stakeholders. Therefore there is a perception coming from the Central Government, HM Treasury[13], that an alternative, quantitative and rationalised risk assessment technique that could be easily understood by all stakeholders would allow greater transparency and scrutiny of decisions. Furthermore, International Civil Aviation Organization (ICAO) has mandated that all Approved Organizations should have a formal Safety Management System (SMS) by April 2012[14]. It is recognized that such a SMS should have a capability to assess an organization's effectiveness in minimizing risk to safety.

In this backdrop this thesis investigates to what extent the risk from human error in a safety critical air transport system could be assessed and quantified to meet industry requirements, focusing on CAW as one area of investigation.

1.1.5 Way forward

Independent research studies by Leach (2005)[15] and Simmons (2002)[16] had attempted to quantify risk from maintenance error. But their methodologies were regarded as too detailed and complex to be practicable as high level management tools. A further,

more directed study by Marsh (2007)[17] offered a methodology to match resources to organization's risk levels, but that too proved limiting in quantification and degree of transparency.

Given the limitations of risk assessment techniques currently used in civil aviation, this study considered Bayesian Belief Networks (BBN) as a way forward. The fundamental concept of BBN has been much researched, and known to have been applied in some sectors such as road traffic management, diagnosis of patients and weapons system effectiveness. Little known applications could be found in civil aviation industry except some academic level research into its potential, Luxhoj (2003)[18].

This thesis will demonstrate a structured path to the design of a risk model starting from the fundamentals of BBN concept and then filling the gaps of knowledge in the design process. The main challenge in this study was how to perceive the concept as the potential solution to the required industrial application, and then to design the model which must capture the complex safety management processes and represent them in the model succinctly. The question of capturing data and validating the model in a CAW environment has also been addressed.

In the absence of relevant public domain literature on the inner workings of organizations responsible for safety management, the researcher's experience in the relevant areas of the aviation sector has been incorporated into this study.

1.2 Aim and objectives of the research program

1.2.1 Aim

The aim of the research programme was to make a contribution to the safety of large commercial air transport through the provision of a novel method of assessing risk attributed to human error in continuing airworthiness.

1.2.2 Primary objective

The primary objective of the study was to design and develop a generic Bayesian model for strategic level assessment of risk due to human error in approved organizations engaged in the continuing airworthiness process of air transport.

The generic model was expected to be validated using field data generated in a continuing airworthiness environment, i.e. data from either an AOC Holder or a Maintenance Repair and Overhaul Organization.

1.2.3 Secondary objectives

Secondary objectives of the research study were to determine:

a. If regulatory oversight of continuing airworthiness organizations could be undertaken on the basis of risk.

b. If approved organizations engaged in continuing airworthiness could utilize the Bayesian risk assessment model to exercise some degree of self-regulation.

1.3 Research strategy

Two strategy paths were considered, one based on hard analysis and the other on soft analysis.

Hard analysis strategy has been recommended where research incorporates experimentation related to physical sciences, and when associated variables are measurable and data can be defined in physical units and dimensions.

Where investigation involves people in real life situations, hard analysis strategy does not work, because it involves people's attitude that is conditioned by feelings, culture and values. Risk assessment at present is very much based on subjective judgment, and expert opinion plays a major role in decision making. Human attitude and mindset are at the very core of the risk assessment process.

This situation initially calls for qualitative methods in order to transit from the existing risk assessment methodologies to a desired quantitative method. How the expression of risk could be represented as quantitative values is another matter, which this research study has tried to examine. Depending on this representation, mathematical laws may be used to analyze data, but in some circumstances the analytical process may have to fall back to qualitative methods and beliefs.

Having considered the two options, it was concluded that the project would follow a soft analysis research strategy.

1.4 Industry support

It was recognized at the outset that consultation with aviation industry was vital to the success of the project. Thus close liaison was maintained with aviation industry, rule-making bodies and subject expert organizations, encouraging them to contribute to this research study from the planning stage onwards. There was direct dialogue with a few selected operators, complemented by collective discussions at the UK Flight Safety Committee meetings and UK FSC Maintenance Sub Committee meetings largely made up of operators and maintenance organizations. Furthermore, the study's progress was reviewed by the primary industrial sponsor and their relevant technical experts every 6-months, and later, by the three industry participants that provided field data.

Appendix 1 lists the public and private organizations that were consulted at various stages of the study, as well as the courses and conferences attended as part of fact finding and research. The field data and supplier information have been desensitized according to the confidentiality agreement.

1.5 Definitions

Technical terms used in this thesis have been defined in the context of the report as they first appear. Any remaining terms and abbreviations have been listed in Acronyms.

This study will consider the safety of those transport aircraft categorized as "Large" whose maximum all up weight at take off (Max AUW at TO) is above 5,700 kg, employed for the purpose of conveying fare paying passengers and cargo under commercial terms and conditions. Findings of this study may be applicable to other categories of aircraft, even though the scope of this study is limited to large air transport.

1.6 Overview of the research study program

The 3-year research programme was conducted in three phases (Figure 1.1)

Phase One. The research programme commenced on the 9 July 2007. At the outset a full time 3-month Industrial Phase was undertaken at the UK CAA. This phase provided an opportunity to understand the objectives, policies and procedures of UK CAA and its relationship to other national and international bodies. The content and

timing of the phase played a crucial role in tailoring the research programme to meet a topical civil aviation industry requirement. The industrial phase was followed by the preparatory work and project planning, literature research and firming up the concept on which the risk model was to be based.

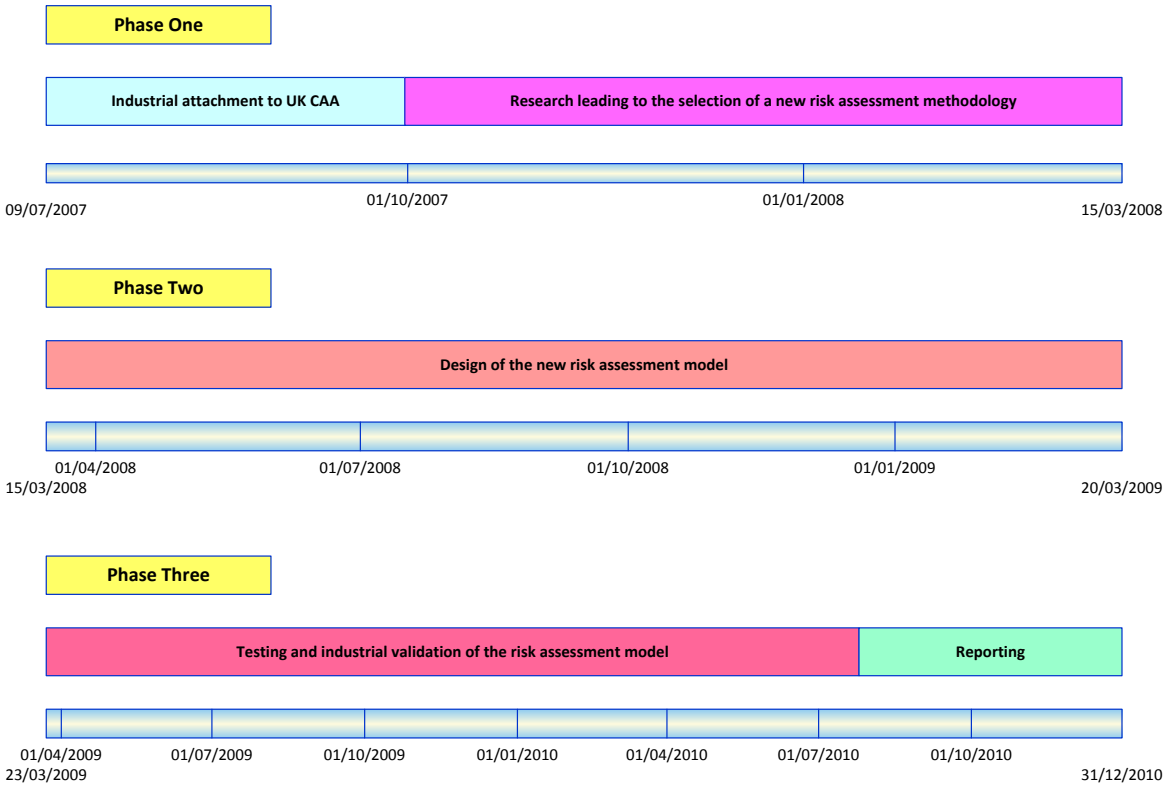


Figure 1.1 – Program phases and timeline

Figure 1.2 outlines the topics studied in order to acquire knowledge on current risk assessment methods in the context of safety requirements, aviation as a business and viewpoints of different stakeholders. Current risk assessment methods were then compared with new assessment methods, identifying gaps and how new methods could bridge the gaps. This process led to the selection of a concept that was taken forward and developed.

Phase Two. The analytical work leading to the design of the model, together with the design itself, was undertaken during Phase Two. This was an intense period of interaction with an industry participant that helped with data required to perform pilot studies on causality, which fed into the risk model. At this stage the program was under close scrutiny by industrial sponsor's technical experts, resulting in continual refinements to the model. Methodology for the design of the model is described in Chapter Five.

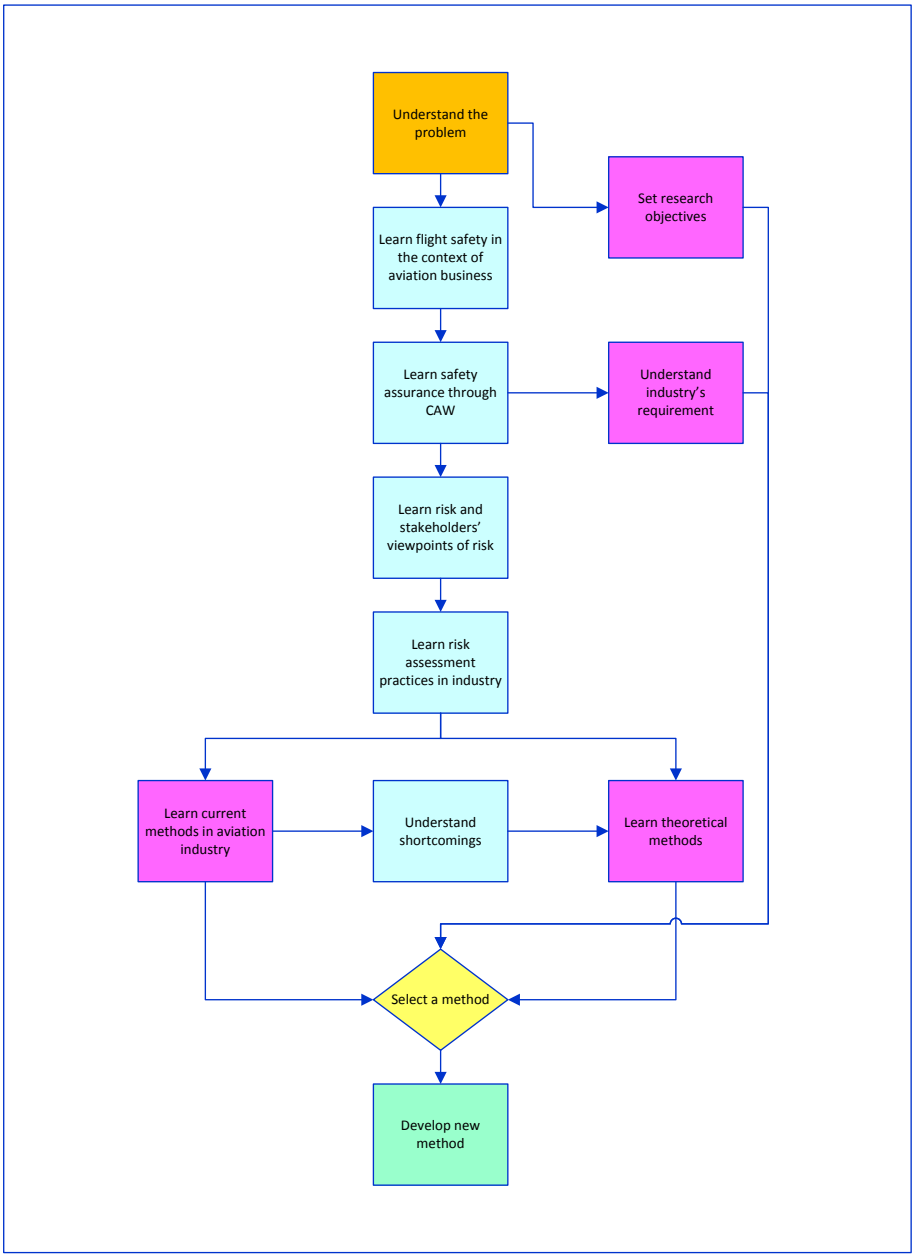


Figure 1. 2 – Flow diagram for selection of new risk assessment methodology

Phase Three. Testing of the model using simulated data was completed during Phase Three, and was followed by a validation trial using industry supplied field data. It was a difficult phase, with operators reluctant to provide sensitive data and shying away from probing questions at a period when the industry was hit by an economic crisis. Nevertheless one operator stayed with the project and provided a full complement of data and the validation phase was successfully completed. Methodology for working with data is described in Chapter Seven.

Chapter Two

Flight safety in the context of air transport business

2.1 Air transport business

Commercial air transportation is a global business that provides an essential service to the travelling public and air cargo industry, making a significant contribution to world economy. This chapter examines the significance of accidents in the context of air transport business, and the way CAW process has evolved to maintain flight safety.

2.1.1 Business turnover

International Air Transport Association (IATA) is an association of traders. The number of its members is fluctuating, but according to data published in the IATA website for 2010, the association was made up of 234 airlines. IATA claims that its members operate around 26,000 aircraft contributing to 94% of the world's scheduled flights. At its peak levels the airlines have been carrying over 2 billion passengers per year, increasing at 4% on average and generating US$ 3 trillion of annual business turnover, representing 8% of world Gross Domestic Products (GDP)[19].

The dedicated air cargo sector in contrast operates around 2,750 air freighters[20], and together with passenger/ freight combinations, this sector has an estimated business turnover of around US$50 billion[21]. At its previous peak level, the air cargo business was expanding at 7% per annum, with a forecast average growth rate of 6% per annum, given stable global economic conditions[21].

In UK, at national level, the air transport industry contributes about £10.2 billion per year to the UK GDP with a projected average growth in air traffic of 4.25% per annum in a steady economic climate as that existed prior to the 2008 downturn.

This magnitude of investment and business turnover could not be sustained unless airlines operate their aircraft safely, and public have confidence in them.

2.1.2 IATA safety statistics

Accidents do happen, but it is necessary to view them rationally, mindful that statistics for major accidents confirm that accident rates are extremely low. According to IATA published data, the lowest ever previously recorded global rate of hull losses for

western-built jets was at 0.65 per million flights[20] in 2006. Since then the hull loss rate for western-built jets has been fluctuating about 0.7 per million flights, until the rate has been further reduced to 0.61 in 2010 according to an IATA Press Release issued on 23 February 2011[114], see Table 2.1.

World Region	Jet/M sector 2006	Jet/M sector 2010
Global	0.65	0.61
Former Soviet Union - CIS	8.60	0.0
Central & South African states	4.31	7.41
Latin America/ Caribbean	1.80	1.87
Asia-Pacific	0.67	0.80
North America	0.49	0.10
Western Europe	0.32	0.45
Mid East & North Africa	0.00	0.72
North Asia	0.00	0.34

Table 2.1 – Air transport accidents rates per million sectors - Global and regional data (Source: IATA)

2.1.3 Cargo operations

A close scrutiny of accident statistics between passenger and cargo sectors points to the air cargo sector as contributing a disproportionate number of accidents to the overall score. For example, during peak operations, of the 28 hull losses recorded against the fleet of 22,738 western-built passenger and cargo aircraft, 13 were attributable to the cargo aircraft fleet of 2,729 aircraft, i.e. 12% of the total air transport fleet[20]. Taken accident rate per 1,000 aircraft, both jet and turboprop cargo aircraft combined have suffered 4.4 times as many hull losses as their passenger counterparts, whereas cargo jets alone have suffered 8.8 times as many hull losses as passenger jets. Eastern built aircraft and other accidents that caused substantial damage to aircraft have been excluded from this statistics in order to simplify this rationale, but even if they were included, the fundamental observation on the greater susceptibility of the air cargo fleet to accidents would not change.

Despite the disproportionate rate of accidents and the slight down turn of the business, the size of the air cargo fleet has been increasing steadily, around 5% per annum at its peak. The increasing demand was being met by older passenger aircraft that continue to be passed down and converted to the air cargo role. Although some new cargo aircraft are built, and some have been entering service, the average age of the cargo fleet of 28-years remained way above that of the passenger fleet of 7-years, according to one report[22]. Utilization of older aircraft in the air cargo sector is a major concern for the integrity of the continuing airworthiness (CAW) process and flight safety. Maintenance and handling operations carried out on these aircraft, predominantly in unsocial hours, and work conducted in developing regions of the world or other outstations where standards and quality controls may be poor are CAW related sub-issues that air cargo fleets experience[22, 23]. Exceeding the max take-off weight and aircraft CG limits may be sometimes linked to unlicensed cargo loaders, irrespective of the operating region.

2.1.4 Risk to communities living near airport

With air cargo operations, there is an added concern to the public and local authorities: that is, they are highly sensitive to movement of aircraft at silent hours, to collateral damage to public and to properties arising from accidents within their conurbations, as well as to the resulting spillage into the environment of dangerous air cargo such as NBC material that some aircraft carry. The crash of El Al cargo Flight 1862 into a residential area near Schipol airport in 1992 and its consequences is a case in point[24, 25]. Black listing of certain air cargo carriers by EASA and FAA is the usual Regulator's response to serious safety concerns of this nature. There is increasing pressure on the air cargo sector to drastically reduce their accident rate, and to take control of potential safety risks unique to air cargo operations in order to make their aircraft safe.

2.1.5. Significance of human error in CAW

What is the impact of human error in air transport and its significance? Plane Crash Info[5] has logged 1,843 accidents that had occurred over a period from 1950 to 2009, whose causations had been identified. Data from about 50-different sources, e.g. NTSB, IATA and Air Claims (a prominent data supplier to insurance underwriters) have been included in the database. Table 2.2 drawn from these statistics attributes 50% of the accidents to flight crew error, 22% to mechanical failure, 12% to weather, 9% to sabotage, 6% to human error and 1% to other causes. The data base qualifies "other

human error" as a mixture of air traffic controller errors, improper loading of aircraft, fuel contamination, and improper maintenance procedures.

From the viewpoint of criticality and number of reported occurrences, the most obvious area for reducing human error is in flight operations, and indeed much effort and resources are invested for this purpose. Although the maintenance error arising rate is relatively low when compared with the rate of error arising in flight operations, the absolute number of maintenance errors may be significant.

Identified Cause	Percentage of total for each 10-yr period						
	50-59	60-69	70-79	80-89	90-99	00-09	Aver
Pilot error	40	32	24	25	27	26	29
Pilot error (weather related)	11	18	14	17	21	17	16
Pilot error (mechanical related)	7	5	4	2	4	3	5
Total pilot error	58	57	42	44	53	46	50
Other human error	0	8	9	6	8	8	6
Weather	16	10	13	15	9	9	12
Mechanical failure	21	20	23	21	21	28	22
Sabotage	5	5	11	13	10	9	9
Other causes	0	2	2	1	0	1	1

Table 2.2 - Air transport accidents causes 1950-2009
(Source: www.PlaneCrashInfo.com)

The figure 6% and 15% human error attributed maintenance incidents quoted in other sources[6, 7, 8] cover a range of consequences from major accidents to low intensity incidents. Though the published data lack clarity in detail, they provide a general consensus on the extent of maintenance related human error contribution in aircraft accidents. They were the reported errors.

It is generally known that a large number of error incidents go unreported because they were regarded as inconsequential. Research into industrial safety has indicated that for every one major or fatal injury there had been 10 accidents involving serious injury, some 30 incidents involving property damage, and 600 reported occurrences with no injury or damage[31]. If these minor risks could be eliminated or mitigated further, then the industry could avert some potential accidents at their embryonic

stage as well as avoiding consequential cost; for example. A return to ramp cost US$ 16,000, flight cancellation US$ 50,000 and an in-flight engine shut down US$500,000[16] in mid-1990 economic conditions. It has been reported that as many as 20 per cent of all in flight shut downs and up to 50 per cent of all engine related flight delays and cancellations could be traced to maintenance errors[32].

Maintenance is only one aspect of a much wider and far reaching safety assurance process, Continuing Airworthiness (CAW) that extends into the management and organizational levels. CAW is only one element in the overall spectrum of measures that assure flight safety in air transport.

In order to understand the way CAW fits into the overall flight safety regime and how the process would have to be represented in the model, this chapter will now take an overview of the conditionality of flight safety, the hierarchical order of flight safety assurance process, and the way CAW is implemented.

2.2 Independent view of accidents in the context of business

Mindful of the inevitable public reaction to the occasional catastrophic air accidents, what would the insurance underwriters reaction to accident statistics?

According to Paul Hayes, Director of Air Safety at London-based consultancy firm Ascend, industry should not be judged on a spate of tragic accidents during a short period of time[26]. *"Today flying is 200 times safer than what it was in the 1950s".* This claim was supported by the statistics for 1950s, when only 31M air travellers flew, there were 39 accidents claimed 799 lives. In comparison in 2008, air passengers numbered 2.6 billion, but the accidents were down to 13 crashes resulting with only 460 casualties.

Despite this encouraging view, it should be stated that over the years the society's perception on the value of human lives has increased, and in the modern world, even one casualty is considered as one accident or a lost life too many. Therefore, whatever the business community thinks, the social and legal obligations of the airlines to the travelling public demands that there should be a continuing effort to increase the level of flight safety.

2.3 Conditionality of flight safety

Flight safety is a conditional phenomenon that works on a system of checks and balances performed on the system by experts. In a system whose stability is

dependent on various interdependent conditions, they must act together to maintain the balance; if not the system would become unstable.

Flight safety has to be assured in each of the four vital, synergistic, functional elements associated with aircraft operations, namely, in the airworthiness of the aircraft, integrity of flight operations, and management of airfield and air traffic operations. The latter two elements, in conjunction with flight operations, manage the ground and air space in the vicinity of an aircraft ensuring that it has a clear passage.

To achieve flight safety in a harmonized manner, everyone who is participating in civil aviation undertakes their operations according to an accepted set of regulations, sanctioned by the law of the country where the aircraft is either registered or operated.

Risk management is implicit in the concept of flight safety assurance, and the system of checks and balances performed by experts as well as by management, at local, national and international levels. At national and international level Regulation and mandates set out the standards to be achieved and, at national and local level, aviation business is regulated by law and compliance with regulation is regularly audited. Within an organization, responsibilities for minimizing risk are diffused down to personnel at all levels including those at the workface. The following sections provide an overview of the flight safety assurance system and how risk management is evolving within the system.

2.4 Flight safety assurance - The hierarchical order

Figure 2.1 is a diagrammatic representation of the top layers of the international and national level flight safety organization and how they are inter-related. It should be read in conjunction with the following sections.

2.4.1 ICAO

International Civil Aviation Organization (ICAO) is the foremost international advisory body that promotes and harmonizes the rules and techniques relating to international air navigation and transport operations. It is important to understand the legal significance of ICAO in UK civil aviation bearing in mind that the effectiveness of UK Regulator is periodically audited by ICAO. UK was an original signatory to the

Convention on International Civil Aviation (generally known as Chicago Convention) signed by 52 nations on 7 December 1944.

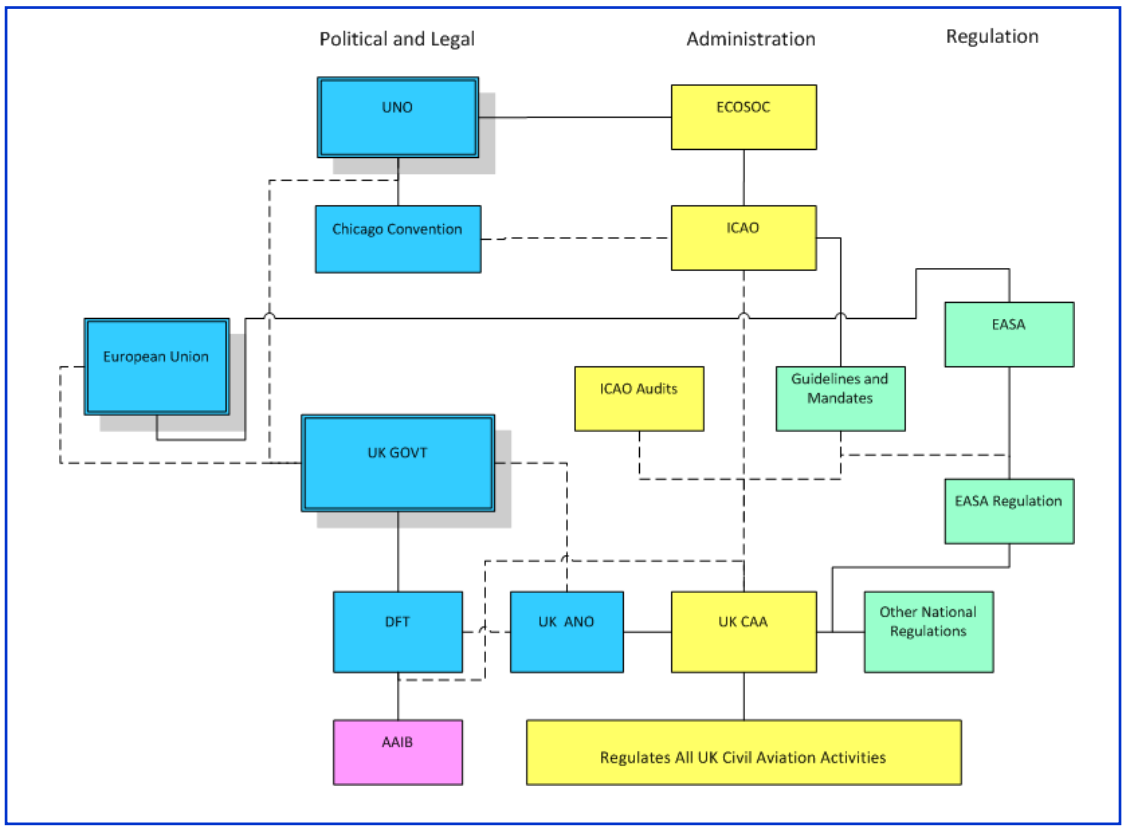


Figure 2.1 - International and national flight safety hierarchical organization

Emerging from this convention, International Civil Aviation Organization (ICAO) was established on 4 April 1947. At present ICAO is a specialized agency of the United Nations linked to Economic and Social Council (ECOSOC). Countries who are members of ICAO have voluntarily accepted to be bound by policies of Chicago Convention and to implement ICAO recommendations and mandates that it issues from time to time[28].

A key strategic objective of ICAO is the development and promotion of aviation safety policies[28] *"in a safe and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated soundly and economically".* ICAO Integrated Safety Management System is one implementing arm of the high-level safety policy.

In the spirit of this strategic objective, national governments have a responsibility to ensure that all aviation activities within their air spaces are properly regulated. Essential elements of such a regulatory process are the technical rules and procedures that constitute the regulations, the legislation that sets out the law requiring

compliance with the regulations, and a Competent Authority to oversee that participants in civil aviation activities comply with the regulations, as well as to enforce the law as and when appropriate.

As a guide for implementing the internationally recognized objectives, ICAO promulgates Standards and Recommended Practices (SARP) as well as various guidance notes relating to safety management. SARP Annexes of specific interest to this research study are:

- Annex 1 – Personnel Licensing.
- Annex 6 – Operation of Aircraft.
- Annex 8 – Airworthiness of Aircraft.
- Annex 13 – Aircraft Accident and Incident Investigation.

2.4.2 UK Air Navigation Order (ANO)

UK has adopted relevant ICAO policy recommendations, currently written into the UK national legislation enacted by parliament under the UK Air Navigation Order[12]. The legislation is applicable to all those who are engaged in civil aviation activities within the UK national air space, and all those UK registered operators who utilise international air space. The ANO sets out legally binding conditions for those who wish to participate in civil aviation activities. It is obvious from the conditions stipulated in ANO that a participant would have to comply with a set of approved safety standards acceptable to the Competent Authority.

Formulation of the air transport policies and legislation that falls within UK ANO is the responsibility of Department for Transport (DFT). It is the government department responsible for strategic transport related issues. The legislation is enacted by the parliament before it becomes the law.

2.4.3 Competent Authority

In the United Kingdom, the role of Competent Authority has been vested on the UK Civil Aviation Authority (UK CAA) generally referred to as the Regulator. UK CAA regulates all civil aviation activities within the UK air space, which fall into two distinct areas: Economic Regulation and Safety Regulation. Economic regulation deals with the commercial aspect of the aviation business. Safety regulation deals with the safe operation of aviation business within UK airspace without risking accidents. To discharge the responsibilities of these two respective roles, UK CAA is organized into Economic Regulation Group and Safety Regulation Group. On behalf of the UK

government, UK CAA Safety Regulation Group safeguards the interests of travelling and non travelling public as well as national and international interests that UK government has agreed to uphold by treaty or by convention.

2.4.4 Safety Standards – The Regulation

As to the safety standards acceptable to the Competent Authority, originally, UK had developed and promulgated safety standards applicable to civil aircraft under British Civil Aviation Regulations (BCAR). Later with a desire to standardize on an international standard, Joint Airworthiness Regulations (JAR) was developed by a number of Western European countries acting together, with JAR gradually replacing BCAR. However with the passage of time and the establishment of European Aviation Safety Agency (EASA) in September 2003 under Council Regulation (EC) 1592/2002 the role of rule making for aviation safety has been transferred from individual nations to EASA. Now UK along with each of the other EU countries takes its share of active participation of rule making under EASA.

Since September 2003, the existing safety regulations applicable to UK civil aviation were allowed to be gradually superseded by EASA regulations within a 5-year transition period completing on 23 September 2008. Now that the transition period has ended, the vast majority of UK civil air transport activities (as well as those in other EU States) are currently regulated in accordance with EASA safety regulations. To be consistent with this evolved status, the Basic Regulation (EC) 1592/2002 has been repealed and replaced by Basic Regulation (EC) 216/2008. EASA regulations now apply to all aspects of design and production approval, airworthiness, continuing airworthiness and training.

Concurrent with the development of safety regulations in Western Europe, other countries outside Western Europe with strong aviation industries have either developed their own set of regulation or have participated in the development of regulation with another strong group of their choice. Most notable are the Federal Aviation Regulations developed in the United States, this being by far the strongest aircraft industry in the Western hemisphere. All foreign registered aircraft must have had the following conditions satisfied before it enters UK air space:

- It should have had prior national level clearance from UK CAA before it enters UK air space.
- Safety regulation under which it usually operates in its home country should be acceptable to UK CAA.

Role of Business Entity	Applicable Regulation	Remarks
Aircraft or component design	EASA Part 21 DOA	Design Organization Approval issued by EASA
Aircraft or component production	EASA Part 21 POA	Production organization approval issued by NAA
Flight operations	Common EASA regulation pending. Meanwhile EU-Ops or JAR-Ops 3 for helicopters apply	Air operator's certificate (AOC) holder certificate issued by NAA of country of registration
Airfield management	EASA regulations anticipated to be promulgated in 2013. Meanwhile governed by ANO Articles 211 and 212, Guided by ICAO Annex 14. Manual of Certification of Aerodromes ICAO Doc 9774. Aerodrome Manual and CAP 168 Licensing of Aerodromes	Approval issued by NAA.
Air traffic management	Pending a common EASA regulation (Single European Sky initiative) regulated in accordance with international regulations and standards applicable to the provision of ATS, including ICAO Standards and Recommended Practices (SARPs) and European Commission legislation. UK CAA Air Traffic Standards Division and ICAO	Approval issued by NAA
Continuing airworthiness management	EASA Part M	Continuing airworthiness management organization (CAMO) license issued by NAA
Aircraft maintenance	EASA Part 145 AMO	Approved maintenance organization issued by NAA
Maintenance Repair and Overhaul	EASA Part 145 MRO	Approved maintenance repair and overhaul organization issued by NAA
Licensed aircraft engineer training	EASA Part 147	Approved training organization issued by NAA

Table 2.3 – Types of business entities and approved organization

2.4.5 Licensing of organizations

An organization (or business entity) that participates in any form of civil aviation must also be legally licensed by UK CAA to take part in aviation activities. The role of the business entities may be varied as shown in Table 2.3. Each entity has to be individually authorized by UK CAA in accordance with the relevant section of EASA regulation before it is allowed to participate in the desired activity.

As part of licensing process, these organizations must prove to the Authority that they are completely fit in their capability and robustness, and that they can fully comply with the requirements and conditions set by international standards. Issuing of a license is conditional upon that approved organization maintaining the initial conditions under which the license was issued. However, from time to time, variations of conditions take place, and then the onus for maintaining the conditions falls upon the organization. If they fail to do so, the regulator has the legal right to intervene and revoke their license to operate.

2.4.6 Licensing of aircraft engineers

Two types of engineers work on aircraft: aircraft mechanics (or fitters) and licensed aircraft engineers.

Mechanics undergo basic training at an approved civil aviation training organization or they could be ex-military personnel who have had extensive, structured aeronautical engineering training in a Service establishment. They may be highly skilled according to their specialization and experience, and are engaged in maintenance, repair and overhaul tasks. They work under the supervision of certified engineers. They can sign for their own work, but their work must be countersigned by a supervising engineer.

Only Licensed Aircraft Engineers (LAE) are allowed to self-certify the work that they have done on aircraft or the work of others that they have supervised. Provided that they have a company approval, they can also issue a Certificate of Release to Service for an aircraft. Licensed engineers have a basic license and aircraft and/or engine Type Rating approved by the National Authority that allows them to exercise these privileges.

In order to reach an LAE status, candidates are required to undergo extensive training in a EASA Part 147 approved training organization, gain practical experience, examined and tested according to the criteria set by EASA Part 66 Regulation. Those who have proved themselves to have acquired the necessary skills and possess good health and fitness may then apply to the National Aviation Authority for the basic license to operate as an LAE, in Categories A, B1, B2 or C license, in accordance with their either mechanical or avionics specialization. A&C and B1 engineers sign for all mechanical tasks on the airframe and engines; B2 engineers sign for avionics tasks.

LAE are allowed to sign for work only if they have a Type rating on the types of aircraft and engines on which they are working. Type rating is obtained after undergoing further training, gaining necessary knowledge and experience, and proving their skill levels to work on the relevant equipment. Usually this training and experience is gained at their employer, an aircraft operator or an MRO, operating a continuing training scheme and certified as qualified to work on the respective equipment according to company internal procedures.

As to the types of work undertaken, line maintenance engineers prepare aircraft for flight using flight servicing schedules such as visual checks of the integrity of the aircraft, replenishment of consumable, rectification of defects reported at the end of the previous flight and any essential out of phase servicing. An LAE must sign-off aircraft "on line".

Base maintenance engineers undertake in-depth maintenance tasks that require aircraft to be taken off from the flight schedule. Depending on the type and depth of servicing and the time taken to complete the tasks, i.e. A, B or C check and their sub-categorization, the work may be undertaken in a hangar at site, or be sent away to an MRO. A mechanic or a licensed engineer may undertake the work, but it must be an LAE who must certify the work and sign off the CRS.

2.4.7 Part 147 Training organizations

Training organizations for licensed aircraft engineers must be approved under EASA Part 147. Some of these organization may exist as independent business units dedicated to industry's training requirements, or if not they may be a part of an existing aircraft operator or an MRO. In the latter case, the training unit would have to be approved by the National Authority under EASA Part 147 for training organization approval procedure.

2.5 Airworthiness of aircraft

Airworthiness of the aircraft is a fundamental requirement to assure flight safety. It is a state that defines the fitness of an aircraft to fly safely in all possible environments and foreseeable circumstances in the role that it was designed to meet[29].

However according to EASA Regulation[30] *"Continuing Airworthiness means all of the processes ensuring that, at any time in its operating life, the aircraft complies with the airworthiness requirements in force and is in a condition for safe operation".*

Meeting airworthiness criteria starts from the conceptual design phase of an aircraft and is carried through all development stages of an aircraft's life cycle until it enters service. Following entry to service, an aircraft's airworthiness must be maintained continuously until its retirement, in order for the aircraft to remain fit for its purpose i.e. for carrying fare paying passengers or cargo.

Prior to its entry into service, an aircraft is required to achieve necessary safety in accordance with closely regulated design, manufacture, reliability testing and production standards. An early development model of a specific type of aircraft that satisfactorily meets the design specification is given a Type Certificate (TC) by an internationally recognized airworthiness authority. The certificate is a design approval issued by the national aviation authority of the country where the product compliance to applicable regulations is demonstrated.

A TC is comprised of the design specification, Type Certificate Data Sheets (TCDS) for example relating to stress calculations and safety factors for structural components or information on fatigue lives, performance data and conditions, operating limitations and numerous other detailed information relating to the performance, integrity, safety, reliability and durability of the aircraft. Usually the TCs are issued for the major assemblies of the aircraft, namely, the airframe, engine and propellers in accordance with EASA Regulation Part 21.

All civil aircraft designed and produced in the European Community are Type Certificated by EASA. A Type Certificate acknowledges that an aircraft has satisfied the design requirements, and is issued under EASA Part 21 type approval procedure. Commission Regulation (EC) 1702/2003 stipulates implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances. EASA Regulation Part 21 provides detail conditions and Acceptable Means of Compliance.

A commercial aircraft's service (or operational life) starts from the point that it is legally permitted by the national aviation authority to be utilized for commercial purposes of carrying fare-paying passengers or cargo. A full production model that has a Type Certificate may be issued with an airworthiness certificate by the National Aviation Authority (NAA) where it is registered. For example, G-YMME is the registration letters of a UK registered aircraft; airworthiness certificate for this aircraft has been issued by UK CAA.

Exact rules and regulations governing the certification of aircraft are very complex. There are many different combinations related to the issue of Type Certificate, issue of Airworthiness Certificate, which country issued the certificates, where the aircraft is registered and where the aircraft is used. All these rules cannot be accurately reproduced in this thesis; relevant EASA or FAA regulations as well as the NAA must be consulted for precise guidance.

Since the process of issuing airworthiness certificate is exercised under the rules and regulations stipulated by legislation of the country where the certificate is issued, the certificate becomes a legal document. With the certificate goes the onus of maintaining the original conditions under which the certificate has been issued to the aircraft operator; this is a legal obligation, such that the operator must not utilize this aircraft for public service or even fly it in the air space of the country, if the conditions under which the certificate was issued could no longer be met for any reason.

2.6 Continuing airworthiness process

The CAW process starts from the time a type certificated aircraft is given an airworthiness certificate to operate in the role for a purpose as declared by the operator. With the passage of time and usage, an aircraft could lose its airworthiness due to variations of its actual state relative to the original conditions, such as wear and tear, deterioration or system defects, rendering it no longer safe to fly. Therefore, one of the many conditions that must be satisfied before an aircraft is allowed to carry fare paying passengers is the continuing maintenance of its airworthiness, to approved schedules, procedures and best practices.

All aircraft in service must undergo continuing airworthiness (CAW) process throughout their service lives to the satisfaction of the regulating authority. This ensures that all airworthiness requirements in force fixed to the issue of the Certificate of Airworthiness are being met and that the aircraft is in a condition for safe operation[29]. It is the responsibility of the authorized operator to ensure that the CAW of aircraft is maintained through the implementation of an approved, structured maintenance process in accordance with EASA Part M regulations. The CAW process maintains the legal validity of the airworthiness certificate.

CAW can be viewed as a system with 2-complementary parts. One part of the system is the timely maintenance of the integrity of the aircraft, physically. The other part is the concurrent documentation of the maintenance activities and associated management decisions, which ensures that maintenance was seen to have been

carried out properly and at the right time. The documentation provides the evidence of legal validity that the process has been carried out as required by regulation, and ultimately, provides the full accountability for the airworthiness of the aircraft before it is allowed to fly. It is the accomplishment of both parts satisfactorily that gives the national authority full confidence on the declared airworthiness state of an aircraft.

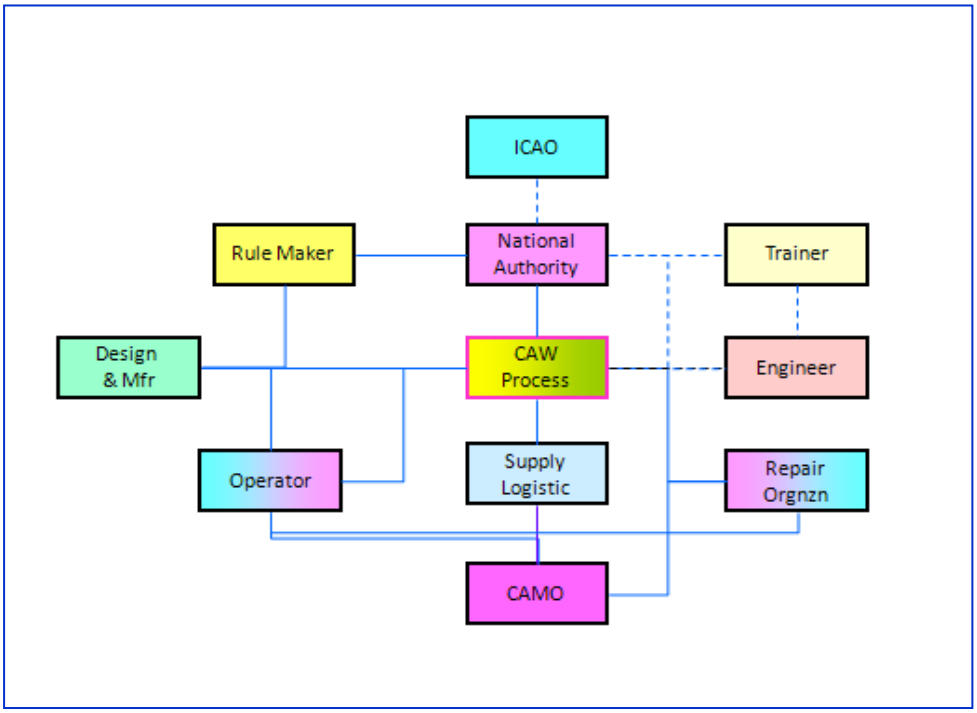


Figure 2.2 – Synergy between organizations responsible for airworthiness

Through these two parts of the CAW process runs the thread of management that pulls together the physical maintenance and documentation, through a system of planning, provisioning of resources, directing and controlling functions. The infrastructure contains all the engineering and logistic support service required to maintain an aircraft's continuing airworthiness to an internationally recognized safety standard.

2.7 Responsibilities of Approved Organizations

The responsibility of the day to day management of the process is vested upon the approved organization that has been licensed to undertake these activities. The Accountable Manager of the AOC Holder is ultimately accountable to the Regulator for any shortcomings and failures of the CAW process.

The approved organization must recognize the conditionality of the issuance of an airworthiness certificate, and then, ensure that the aircraft is maintained to a standard agreed by the authorities. If not the license to operate that aircraft might be revoked. The approved organization must set up a maintenance system and its management.

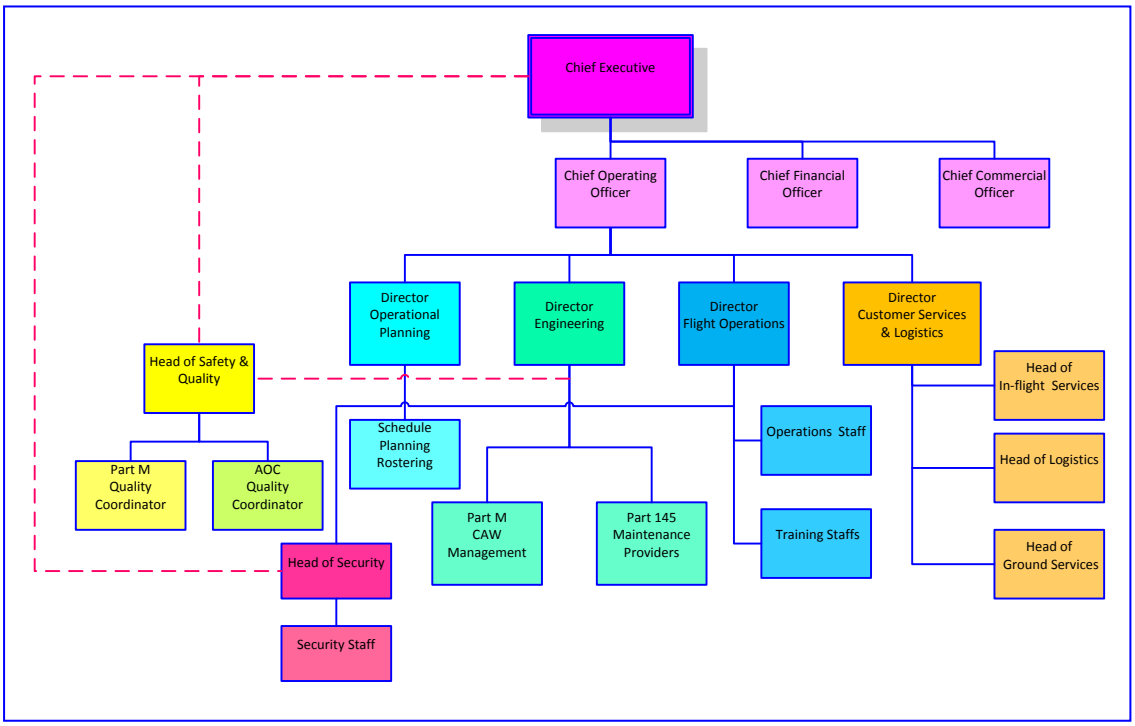


Figure 2.3 –Organizational structure of a typical airline top-level management
(Source: Industry participant)

The management system would have a maintenance operation component, and auditing, monitoring and controlling components that provide information to the Head of the Organization, usually it's CEO. The AM/CEO should have full financial powers of resourcing the CAW process that meets the original conditions. The way CEO's powers are delegated down the management structure is shown in Figure 2.3 demonstrated here with the use of management infrastructure of a regional air line.

2.8 Implementation of CAW process and synergy between AOs

In the UK any business entity that wishes to operate air transport under commercial terms must obtain a license, a legally binding approval from the Competent Authority which is the National Aviation Authority. In the UK this authority is vested on the UK Civil Aviation Authority.

Establishment and operation of these organizations are regulated by national authorities, in accordance with safety regulations formulated and promulgated by European Aviation Safety Agency (EASA).

2.8.1 Approved organizations

Regulations are published as reference documents, divided into parts as applicable to different approved organizations according to their roles. Organization licensed to operate under relevant parts of EASA Regulation are usually designated by the Part Number/ or Letter. Thus:

- EASA Part M – The airworthiness management arm of an Aircraft Operating Certificate (AOC) Holder.
- EASA Part 145 – A provider of aircraft maintenance services under contract to a Part M Organization.
- EASA Part 21 – Aircraft Design Organisation and/or Production Organization that continues to provide post design/ production services to AOC Holder.

This study identifies Part M and Part 145 as core organizations because they have the greatest influence on the airworthiness of the aircraft on day-to-day operations.

This is a good opportunity to examine the synergistic relationship between various organization involved in the CAW process, placing the aircraft operator in focus as the principal player.

Commercial flying operation is undertaken by an AOC and Operating License Holder. The airworthiness of the aircraft is monitored and assured by a Continuing Airworthiness Management Organization (CAMO) in conjunction with a maintenance provider. CAMO is a Part M approved organization and the maintenance provider is a Part 145 approved organization. Part M and Part 145 organizations may be established either as an integral part of the aircraft operator or be contracted out. The intended end product of the joint activity between these 3-organizations is the provision of a safe flight.

2.8.2 Management and operation of CAW process

Management of continuing airworthiness of the aircraft is done according to an Aircraft Maintenance Programme (AMP) agreed between the AOC Holder, being the user customer, and the Part 21 DOA/POA who is the supplier of the aircraft and

systems. Part 21 DOA/POA is usually identified as the Original Equipment Manufacturer (OEM). AMP must be approved by the Regulator as meeting safety requirements, but its implementation and updating according to operational or technological changes is the responsibility of the AOC Holder.

The day to day engineering operations are coordinated by a Maintenance Operations Control Centre (MOC) that usually functions alongside and in harmony with Flight Operations Centre. Part of the MOC manages all the aircraft on line, either at the parent base (or the hub of operations) as well as on-route. Another part manages those aircraft on Base Maintenance either on site or at an MRO. Priorities in the generation of aircraft on line are decided routinely by the Controller of MOC and equivalent Flight Operations Controller, and exceptionally by Director of Operations in consultation with Director of Engineering.

Engineering operations to prepare aircraft for flight are carried out on the line. The Part M organization coordinates the engineering operations by monitoring the CAW status of each aircraft, undertaking advance planning, directing and controlling the maintenance tasks through interdepartmental work orders as requirements arise.

The Part 145 organization, i.e. the maintenance provider, undertakes the work stipulated by the Part M organization. If these are separate business entities, the information flow process, task loading and other logistic aspects of task requisition and implementation are subject to interface contracts between the organizations. Quality and Safety of the work is audited by the Quality and Safety Management Services of the AOC Holder, whose head reports directly to the CEO of the AOC Holder.

Other external organizations provide services to Part M and or Part 145 organizations. The most important is the Design Authority (DA) for the type of aircraft operated by the AOC Holder. The DA is invariably the EASA Part 21 DOA for the aircraft, and most likely the principal manufacturer of the aircraft as well; in the latter case they are also the Part 21 Approved Production Organization for the aircraft, i.e. Part 21 POA.

Further to the provisioning of an AMP, there are numerous other responsibilities vested on a Part 21 organization by Regulation, e.g. to provide post design support facilities for the product. Usually known as product support service, AOC Holders become fully dependent on Part 21 organizations for design information and integrated logistic support, material and information flow. Examples are: engineering skills and training requirements, maintenance spares, ground support equipment,

tools and test equipment, ways of dealing with previously unknown defects, their investigation and disposal and prevention of recurrence, modifications, impact of operating changes on durability and maintenance etc. In this respect EASA Regulation Part 21 lists the responsibilities of Part 21 approved organizations. The information exchange process is written into commercial interface contracts between the Part 21 organization and the AOC Holder or if not the delegated Part M organization.

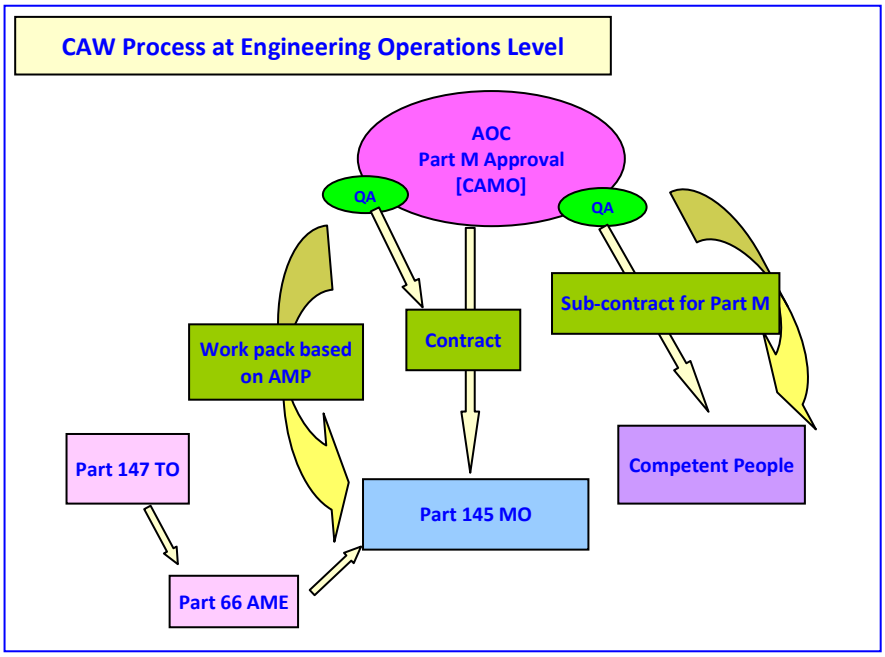


Figure 2.4 – CAW process at engineering operations level

Heavy maintenance of aircraft, such as C-Checks and modifications, is normally undertaken by specialized Part 145 approved Maintenance, Repair and Overhaul Organizations (Part 145 MRO). This work is contracted out by AOC Holders, task requirements are defined by work packs raised by Part M AO, and the quality of end products is progressively audited by the AOC Holder's Quality Management System (QMS). The work and information flow and the terms of engagement are controlled by interface contracts. Part 21 support requirements for those aircraft undergoing Part 145 MRO maintenance are either referred back to AOC Holders or are facilitated through supplementary contracts that enable Part 145 MRO to directly access Part 21 AO.

Investigation of previously unknown defects that arise in service and recommending solutions is an important regulatory and flight safety requirement The reporting of such defects to the Part 21 DOA is the responsibility of the equipment user. If the defect is associated with a Mandatory Reportable Occurrence (MOR) defined under UK CAA CAP 382, then the AOC Holder must raise the Occurrence Report and in doing

so would bring UK CAA into the investigation. Defects that have an impact on the Type Certificate and configuration of aircraft would invariably be referred by Part 21 AO to EASA (who normally issues the Type Certificate for aircraft designed and manufactured in the European Community) and any solutions would have to be approved by them before promulgation, e.g. either as an Airworthiness Notice or an Airworthiness Directive. Long term or permanent solutions to in-service defects might be equipment modification, procedural changes or introduction of new maintenance activities incorporated into the AMP.

EASA Part 147 Training Organizations (TO) should be mentioned here as they are the licensed organizations authorized to train engineers that maintain aircraft. Certainly Part 147 organizations play a key role as they are expected to output good quality engineers; the standards set by TO are reflected by the quality of engineers who work on aircraft and their standards. The standards are particularly relevant in the context of human factors and the susceptibility of engineers to human error at work place. Some AOC Holders have their own integrated training organization that provides initial training for in-house trainees and continuation training for engineers already employed by their associated Part M and Part 145 organizations; they may be authorized to outsource training facilities to other customers.

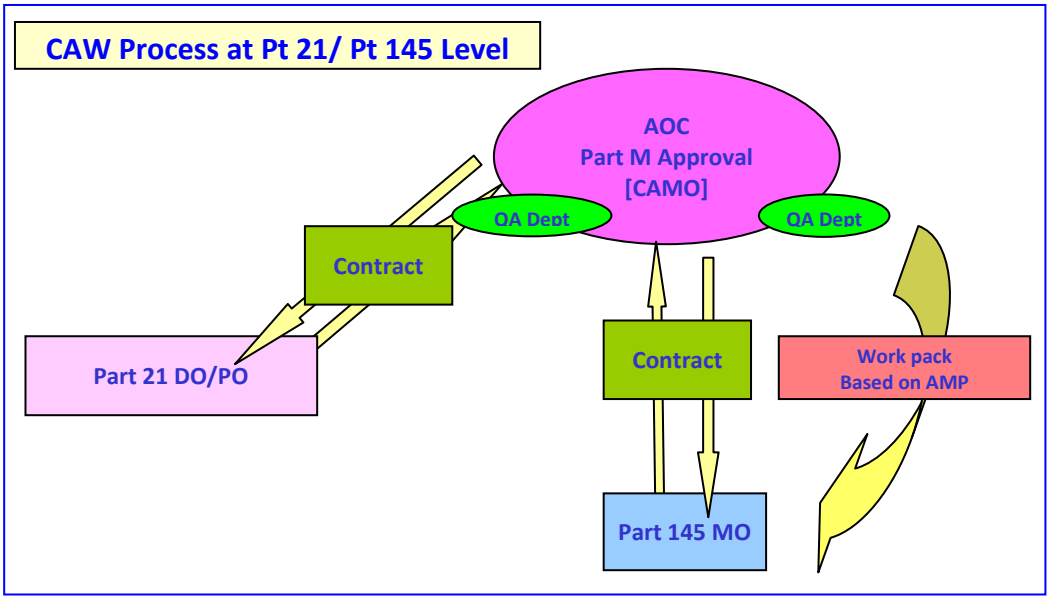


Figure 2.5 – CAW process interaction between Pt 145 Pt M and Pt 21 AO

Figure 2.4 to Figure 2.6 illustrate the synergy between various members of the core group and their lines of communication. Note that communication and interaction on professional and technical issues between approved organizations are controlled by interface contracts. Although EASA regulation spells out regulatory responsibilities

between these organizations, they are implemented as a commercial service with both financial and legal implications to parties concerned.

There are other peripheral organizations involved in support of the above mentioned approved organizations, such as stand-alone continued airworthiness management organizations (CAMO) component overhaul organizations, spare parts suppliers and various other logistic support contractors in supply chains. Some of these are directly regulated by CAA under EASA regulations, e.g. CAMO. Others, e.g. out source for technical personnel, may not be directly licensed by CAA, yet still regulated under the rules applicable to the parent organization to whom the services are provided.

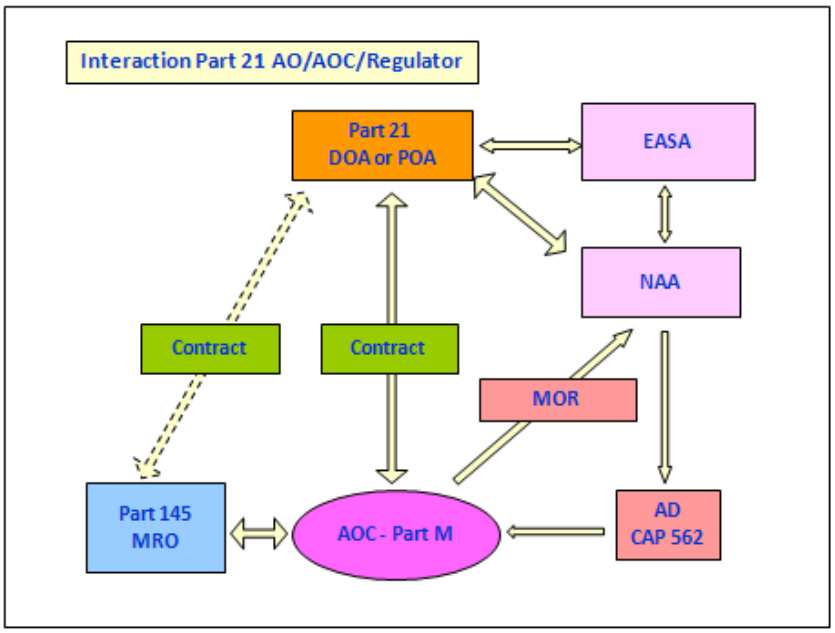


Figure 2.6 – Synergy between AOC Holder Pt 21 AO and Regulator

2.9 Safety Management System

Hitherto, the role of flight safety auditing, monitoring and reporting change had been vested on the Quality and Safety Department of an approved organization. However over the recent years ICAO, through amendments to relevant ICAO Annexes, has mandated the establishment of a Safety Management System (SMS) in approved organizations.

According to UK CAA guidance notes, Safety Management System is described as "*an organized approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures*", and that it will be based on ICAO Document 9859 – Safety Management Manual. The new concept of SMS would

introduce a new tier of flight safety management and make significant structural changes to the existing management of an organization's flight safety assurance functions. Thus an SMS would be introduced to coordinate and integrate safety management across all departments that contribute to flight safety. The existing Quality Management System will be retained to monitor compliance with and adequacy of procedures required for safe operational practices and airworthiness of aircraft.

Safety management systems have already been established in air traffic control and airfield management environments as per Annex 11 and Annex 14 respectively. Flight operations (Annex 6) and maintenance (Annex 8) environments are required to be fully compliant by April 2012.

EASA implementing Rules for Management Systems and Authority Requirements will contain a requirement for an ICAO-compliant SMS.

2.10 Risk to airworthiness

A quality management system working in conjunction within the framework of an SMS should detect sources of errors that undermine airworthiness and recommend methods of eliminating them. Observing the distribution of sources across the infrastructure of an organization as described below, it becomes clear why it is necessary to have an SMS organization that has the power and authority to force through safety policies and coordinated interventions that affect the entire organization.

The most obvious source is the human-machine interface of engineering operations[1]. Often, errors that occur at the work face have a bearing to time pressures coming from flight operations and business managers. Errors also occur in the technical and logistic infrastructure (supply, organizational and management) that supports engineering operations. Interface contracts between approved organizations that control information flow, work orders, deliverables, and their safety and quality, are known to be sources of contributory causal factors that lead to human error. This is evident in some of the case histories outlined in Appendix 7 (A/08/001) and Appendix 13 (ID 27).

Errors at planning, resourcing, directing and controlling of maintenance activities could undermine the defence mechanism that prevents the consequence of a prior error; see Appendix 7 (A07/025, A07/027). With cost conscious managers looking for

cost savings, business focussed decision taken by managers are known to have progressively undermined existing defence mechanisms[9, 10]. In some situations, it has been the systematic failure of defence mechanisms that ultimately caused an accident, which in some cases ended up as catastrophic[102].

An SMS should have a capability to discriminate between the relative importance of different types of error, consequences and interventions in order to help AM/CEOs prioritize investment decisions. This is because, not all errors lead to major accidents. They have different consequences, since the magnitude of the errors themselves are not necessarily proportional to the consequences. For example, it is quite feasible for a prominent error to cause an insignificant outcome, whilst a small error might lead to a big consequence[10]. As postulated by Reason[1], it is the timely defence that would or would not avert the consequence.

In the current economic climate where available funds are limited, safety requirements would have to compete with other investment demands that might be just as important to the business. Such competition demands a greater accountability and justification for the investment, which an SMS could provide as an impartial organic arm.

2.11 Business and Commercial Risk

In addition to safety regulations, the businesses must also comply with finance and economic regulations set by the National Authority. Every business carries a business risk, but that aspect is not addressed in this study even though business risk is acknowledged. The study is mindful of the impact of safety on business risk, as well as the impact of funding on safety. This balance between safety and funding is critical to the survival of the business as well as to the aircraft and people who fly in them.

One aspect of the national authority overseen economic regulation is the provision of insurance to cover third party risks in the event of an accident. Although this study has not addressed insurance issues, it has recognized the importance of insurance as a method of underwriting the consequences of incidents and accidents. For example, a CEO with a short range planning horizon might consider that it might make more economic sense to him if flight safety risk attributable to human error be covered by insurance instead of a long range strategic planning and investment within his organization.

2.12 Regulatory oversight

In the UK, all organizations that participate in aviation business must be approved by UK CAA. Part of the approval process is an assessment of the capability of the organization to comply with the safety regulations. Furthermore each organization is regularly audited by CAA to ensure that they continue to maintain the approval conditions.

That aside, there is also an onus on the national Regulator to carry out periodic audits and oversight inspections of approved organizations that have been licensed to participate in civil aviation activities. This arrangement takes into account the variability of an organization's own responses to any change of state of the organization or the airworthiness of aircraft. For instance the attitude, safety culture or economic situation of the organization and its management may indicate the way resources are allocated to maintain safety standards.

On its own part, the Competent Authority, through oversight inspections, routinely monitors the performance of approved organizations against the regulations to ensure that regulatory standards are maintained. Approved organizations are advised of any observed variations that could have an adverse impact on safety, and these shortfalls would then have to be corrected in order to maintain the validity of the organizations license. In extreme cases, where corrections were not made after repeated warnings by the Competent Authority, it has the power to revoke the license from an offending organization according to the technical and legal powers delegated to the authority.

Under current CAA SRG procedure all regulatory aspects of an approved organization in the UK are subject to oversight inspection over a 24-month period, which is the minimum frequency that has been recommended by ICAO. This process is repeated cyclically.

2.13 Linking research studies to industry requirements

Given that there is always some form of risk assessment in use in air transport operation and management, the latest drive for an innovative assessment method has come from two specific foreseen industry requirements. These are:

a. The ICAO mandate for Safety Management Systems[14].

b. Regulatory risk-based oversight (RBO) as recommended in the Hampton Report, which is part of HM Treasury initiative into Better Regulation[13].

2.14 ICAO mandate on Safety Management System

The AOC Holder is responsible for airworthiness and it follows that Part M and Part 145 approved organizations that fall within an air operator's area of responsibility should comply with the mandated SMS requirement.

The key features of the SMS are that the system must be formal and structured, and the principles and method of implementation of SMS must be documented. SMS should contain the elements: Risk Management Process, Safety Case, Hazard Identification, Risk Assessment, Risk Reduction and Mitigation.

Thus it is clear that there should be a means of complying with risk management process, in which risk assessment forms one element and for which assessment tools may be required.

2.15 Risk Based Oversight Concept

Risk based oversight (RBO) concept is a key recommendation in a report produced by Philip Hampton[13], Head of a UK HM Treasury appointed committee tasked with findings ways to reduce the administrative burden experienced by regulated industries by promoting more efficient approaches to regulatory inspection and enforcement. The committee, set up in 2004, was required to examine the practices of a wide swath of UK Industries and regulators, including UK civil aviation industry and CAA.

In his report published in 2005, Philip Hampton made a number of recommendations, all of which have been fully accepted by HM Treasury[33]. It is understood that the recommendations would be passed down to the relevant Industries and Regulators for compliance after they have gone through a legislative process. Formulation stages of legislation will include a process of consultation with the stake holders of the industry and seeking consensus through negotiation, for which HM Treasury's Better Regulation Executive (BRE) has the administrative responsibility.

Whatever the regulation that will stem from legislation based on Philip Hampton recommendations could then form a strategic requirement on the way regulatory

oversight would be undertaken. If that were to be so, then UK CAA should be prepared to meet this challenge by developing a capability to assess and quantify the risk levels in the industry that it regulates.

2.16 Desirable criteria for a risk model

Given these two formal and hierarchical needs, together with an organization's desire to prioritize investment on flight safety, this research study starts with the premise that one single risk assessment methodology based on quantitative techniques could serve both purposes.

Although there was no formal specification for an assessment method, the study was able to focus on a wish-list of criteria suggested in Philip Hampton Report[13]. It envisaged that a new methodology for risk assessment should:

- Be open to scrutiny.
- Be balanced to include past performance & future potential risk.
- Use all good quality data.
- Be implemented uniformly & impartially.
- Express simply, preferably mathematically.
- Be dynamic and not static.
- Be carried through to funding decisions.
- Incorporate deterrent effects.
- Include an element of random inspection.

According to the initial remit from the sponsor a model incorporating a top down analysis was the management's preferred solution to risk assessment. Nevertheless, a bottom up process-review may be necessary to ensure that any remaining gaps in the defences missed during the top down process are detected and dealt with.

The quantitative risk assessment method ought to be simple and practical, its functionality transparent and, in order to economize, preferably based on the sort of input data that is usually collected in current error management processes.

Chapter Three

Literature research - Risk assessment practices in civil aviation

3.1 Introduction

This chapter will examine in depth the concept of risk in general and how it is applied to civil aviation, as well as reviewing current risk assessment practices in UK civil aviation.

3.2 Risk assessment in the face of conflicting needs

Hitherto, the air transport industry was guided by the ICAO definition of risk given in SMM. This states that risk is the assessment expressed in terms of predicted probability and severity, of the consequence(s) of a hazard, taking as reference the worst foreseeable situation[38]. It qualifies the definition by providing a conditional reference point, i.e. "worst foreseeable situation" from which risk ought to be assessed.

The "worst possible situation" is difficult to define. It depends on the collective historic knowledge. An individual engineer or surveyor would have only a small fraction of that knowledge and his own experience. Safety engineers are required to utilize the ICAO definition but the feedback that the study received from them was that if they strictly apply this definition, then the assessment could be too severe and they would get into conflict with the operator's business managers. This brings this study face to face with the main issue that need to be addressed, i.e. a way of determining risk that is acceptable to both safety experts and those who are interested in the commercial aspect of the air transport business.

The conflicting demands faced by the State, the Regulator and the aircraft operator in determining if risk is acceptable has been succinctly put in Figure 3.1. Increasingly under pressure to generate more revenue, the State might view the merits of increasing air traffic and activities of associated aerospace industries and support industries such as maintenance, logistic, training, , and hospitality.

At the same time the State may be concerned by the need to ensure public safety, as well as to minimize the negative impact on the environment caused by increasing air activity. Therefore the government may have to increase regulation in some areas such as environmental pollution, whilst de-regulating in others, for example relating to Open Sky policies. The aircraft operators would like to increase its turnover, to

maximize profit and minimize costs. They would like to see existing regulation minimized, and certainly costs associated with them curtailed.

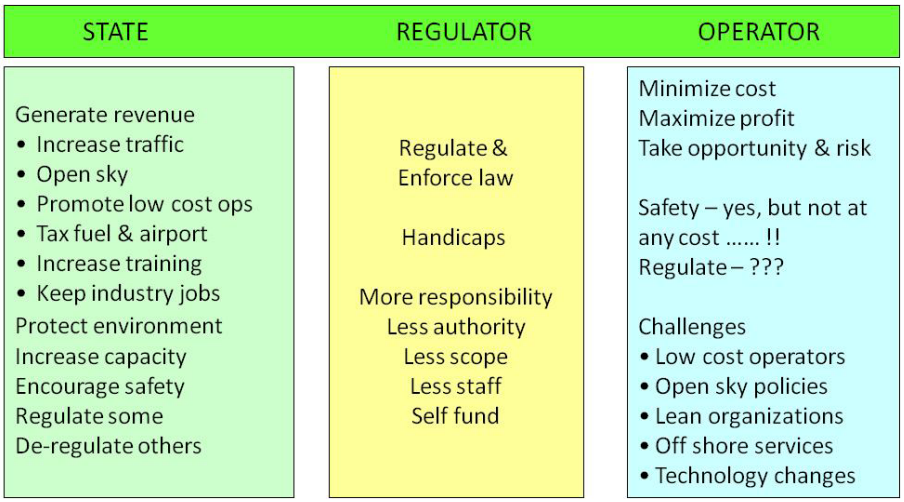


Figure 3.1 – Conflicting demands between the State, Regulator and Operator

It is in this context that the operators are looking for some relaxation of existing regulation, especially in the way the regulation is administered, with an eye for cost saving. Caught between the government and the operator, the national Regulator has been forced to find the right compromise between safety needs and cost needs, while burdened with the responsibility of generating the income necessary to maintain its capability, i.e. to discharge the duties that the government has delegated to it. It is the government policy that the cost of managing and maintaining CAA's services must be paid for by the users of such services.

Despite their widely differing business objectives, they all agree on the need for flight safety as a common denominator. Therefore a possible way forward is by developing a capability to assess risk that is not sensitive to personal interpretation and judgment. Quantitative assessment of risk provides an opportunity to assimilate the state of flight safety from another perspective and then to apply this knowledge to sensible management decision making process.

It should be said at the outset that the availability of a quantitative risk assessment technique in itself would not eliminate flight safety risk. It is the decisions made by top level managers that will increase or decrease the flight safety risk from a strategic point of view, because they are the ones who have the capability to either resource or introduce far reaching policy decisions that affect the entire organization. Quantitative information on risk helps to make better decisions in so far as critical

input risk data is concerned; however at the end, management decisions may be taken, having given due regard to all other conflicting demands.

3.3 Conditionality of the outcome and risk - Data

To what extent the risk due to human error could be tolerated in a safety critical air transport system? To answer this question, it is necessary to have better intelligence on the degree of uncertainty of the outcome, where the outcome itself is conditional. Then it might be possible to control the uncertainty. Most people forget the conditionality of "outcome" and in turn of "risk". Therefore, first, conditionality of the outcome should be examined, i.e. the circumstances under which an outcome occurs. More information on the conditions for different outcomes may be necessary, such as hazards that prevent the achievement of objectives, how often they manifest themselves, what were the human errors if they were the threats, and if they were primary or secondary causal factors etc. Quite simply, associated with each outcome, there should be a comprehensive set of data detailing the environment and circumstances in which the outcome occurred.

3.4 Mechanism to assimilate the conditions - Method

Once conditions are known, then there ought to be a mechanism to assimilate the net effect of multiple, variable information. The natural process of assimilation takes place in the brain and in the mind of those who face these conditions. Unfortunately, the complex thinking process of risk assessment is not fully transparent to others, even though an expert or a careful observer could detect some outward symptoms of the person's thinking and impending decision. Given this limitation, there is a social demand for greater transparency of the decision process relating to risk taking, because everyone wants others to be accountable for their decisions and actions. Accountability is very much in the forefront when it comes to any accident, large or small, where the legal liability for the outcome, payment of compensation and corrective actions, has to be determined. The mechanism for assimilation of information on conditions is the key to determining accountability for risk, and is a very important element in risk assessment.

3.5 Expression of risk - Output

Finally, there is the question of the output from the risk assessment methodology and the way it is to be expressed so that everybody can have a meaningful, common understanding of what the result conveys. Most risk assessment methods output the

result in qualitative form, such as risk being High, Medium or Low. Sometimes the same result may be given with a better resolution such as the chance of a certain hazard occurring leading to a catastrophic failure as extremely low, or very high. Again these qualitative words convey different meaning to different recipients of information according to their experience and imaginations.

Converting a qualitative measure to a quantitative has always being the general convention and, wherever this is possible and practical, the society has adopted such convention because they are more meaningful to them especially when used for comparison. Units and dimensions, used in daily life or in scientific work are prime examples. Similarly, it is desirable to express risk on a numeric scale. However the current methods of converting qualitative expression of risk to quantitative form are themselves subjective and therefore the exchange rate may be variable between different risk experts. This is an undesirable state. What is required is a more rational and unbiased system of conversion that does not rely on individual experience and fear.

3.6 Definition of risk

It follows from the foregoing analysis that a risk assessment method requires information on the probability of the hazard occurring, a measure of the consequence, and a method of combining these variables.

The most universally accepted mathematical formula that combines loss or severity of consequence with the probability of its occurrence is:

$$R_i = L_i \,.\, p\,(L_i) \qquad \textbf{3.1}$$

This formula is valid for one known consequence, where L_i is the severity of consequence, and $p\,(L_i)$ is the probability of consequence.

For a series of events from i = 1 to n, the expression for the total risk could be rewritten as,

$$R_{total} = \sum_{i=1}^{n} L_i \,.\, p\,(L_i) \qquad \textbf{3.2}$$

This is the summation of risks for independent events.

In most safety sensitive industries such as nuclear, rail and air transport, where the usual measure of safety is through risk assessment, the same equations as above apply. However L_i would be read as the severity of consequence and p (L_i) as the probability of the hazard occurring that leads to the consequence.

Where the events are not independent, p (L_i) becomes more complicated as it would be necessary to establish conditional probabilities. Then this simple formula would not apply. This is the situation with complex processes such as continuing airworthiness, where steps of a process system are numerous and interdependent on what happens elsewhere in the system. This research study will especially address this type of complexity.

It is axiomatic that the methods of measuring the consequences and the probability of occurrence form the key to the way risk is expressed. Obviously both these quantities could be expressed in quantitative terms as well as qualitative terms, depending on what is at stake. For example if a person's life or someone else's reputation is at stake, it may be difficult to put a value to it, though more often than not law courts end up with putting an agreed monetary value to it during compensation claims. Loss of impersonal assets such as aircraft or property on the ground, or loss of earnings could of course be easily quantified.

Similarly, the probability of an event occurring could be quantified if there is sufficient amount of data that represent the past experience. However if data is not available, then the probability of occurrence would have to be estimated or if not best guessed using expert opinion. Often the expert acts without sufficient data at hand, and his experience may be based on either hearsay or the personal experience of a very few similar events. Thus judgment may be clouded, and at best be expressed qualitatively.

3.7 Quantitative risk assessment

It follows from the foregoing discussion that risk assessment is the determination of the qualitative or quantitative value of the risk associated with a measurable threat or hazard that could arise at a specific situation. If risk is to be assessed quantitatively, then it is necessary to calculate the two components that form risk, namely the probability of the threat (or hazard) and the magnitude of the potential loss or consequence.

3.8 Current risk assessment methods in civil aviation

This chapter from here onwards will examine the way risk assessment is implemented in civil aviation at present. Table 3.1 identifies some of the risk assessment

opportunities and methods encountered in UK civil aviation. Some of them are discussed under this literature survey.

Method	Role	Application	Objective
ICAO Audits	ICAO conducted audits of national civil aviation policy and safety regulation infrastructure	International level audits of each ICAO member nation	To monitor effectiveness of national infrastructure's compliance with ICAO international standards.
IOSA	IATA conducted operational safety audit	Flight operations	An IATA managed commercial audit service chargeable to customer (air operator). It covers the audit of maintenance operations and organizations that come under ICAO Annex 6.
Regulation	Oversight inspection and audit	Conducted by NAA on all approved organizations	Mandatory compliance with regulation. Legally binding
SMS	In house safety management	All operations	ICAO mandate current, but not a legal requirement in UK
QMS	Administrative process to international standards ISO 9001/9002, TQM or six-sigma	All operations	Quality audits assure infrastructure, rules and procedures are in position and being complied with by lower formations. Quality control – routine audit of quality of work at work face done locally
MOR	Mandatory Occurrence Reporting system.	All operations	Monitoring performance. MOR rate is currently used as a KPI for measuring effectiveness of flight safety management.
MEDA	Analytical tool to manage HF based reported errors.	Maintenance operation	Classify reported errors, to identify and determine corrective actions
MEMS	Formal HF based error reporting	Maintenance operation	Data collection and analysis. To monitor in house performance and prevention of future incidents.
CHIRP	Confidential reporting outside established MOR and MEMS procedure	All operations	Data collection and analysis to identify sensitive causal factors that prevent or suppress normal reporting
FMEA	Analytical technique	System or product design	Increase system reliability, reduce life cycle costs minimize risk to ALARP.
MSG-3	Analytical technique	Designing maintenance systems	Increase system reliability, reduce life cycle costs and aircraft downtime, and minimize risk to ALARP.
SHEL	Generic analytical model for human factor base error incidence	System design or operation	To identify sources of error leading to HF based failures.

Table 3.1 – Risk assessment - circumstances, systems and techniques

3.9 Circumstances for risk assessment

Risk assessment may be undertaken at different circumstances:

a. Tactical planning as part of day to day operations, as situations arise.
b. Meeting regulatory requirements as undertaken by the Regulator.

c. Strategic planning as a part of safety management and better resourcing, usually undertaken by an organization's higher level management.

Tactical risk assessment methodology involves the analysis of a given situation to identify the hazards, consider the potential consequences and severity as well as if the hazard is likely to materialize and lead to an incident, and then make a judgment if a significant risk exists or not. Conversion of feelings, opinions and judgments is based on a definition that outputs a number. It could be said with certainty that nobody resorts to a calculator or a computer to make an on the spot tactical risk assessment and decision in the middle of an engineering or flight operation. Decisions are taken on the basis of the best experience of the people involved. More often than not, time pressure is involved in tactical risk assessment.

In contrast, risk assessment for strategic planning is done under more relaxed working conditions. There are more opportunities to exercise a higher degree of resolution of hazards, consequences and their severities and probabilities. Even so, assessment technique is largely subjective in the current state of the art. Conversion of subjective judgment to numerical values may be using simple linear scales and pre-defined criteria, as explained further on this chapter.

Assessing risk for regulatory purposes is quite different. Here it is a question of how well and closely an organization complies with prescribed rules and regulations. If there is a failure to comply, or if the rules are breached that becomes a fault. The fidelity of the individual or the organization is in doubt, and the risk arises from this uncertainty over the organization's reliability and the trustworthiness rather than from the fact if the situation really posed a risk to flight safety. The gravity of the fault may affect the penalties and corrective actions.

3.10 Risk assessment in tactical planning and operations

Risk assessments in tactical planning and operations are undertaken by air operator or its maintenance organization. These opportunities arise very frequently. Assessments are done by specialists of the organization such as flight crews, engineers and their line managers. Their work may be assisted by diagnostic software for the aircraft systems involved. If the decision process is error free or not, is left entirely to the integrity and fidelity of the individual decision makers.

Ideally the need to assess risk by specialists should not arise, if prior integrated logistic support planning has been undertaken perfectly, if all the necessary resources have been provisioned and if personnel follow correct procedures promulgated under safety regulation. But in life, nothing is perfect and often new unknowns, in the form

of shortcomings, come into light, which need addressing. Then, specialists involved might have to make an assessment of safety risk on which a decision has to be taken. Here is an example of such a situation.

3.10.1 Case study in tactical risk assessment – safety vs cost

A defect in the form of a smouldering cable was discovered on an aircraft that was en-route, which rendered part of a system inoperative. Rectification of the defect was outside the capability of pre-planned en-route engineering and logistic support arrangements. The captain of the aircraft reported to the home support base that the affected part of the system was not in the aircraft's Minimum Equipment List (MEL) and could be disabled. But he suspected that disintegrating insulation might be the cause, and even if the circuit was disabled, a very small fire risk could exist from the adjacent cables of the loom through which other essential systems were powered during flight. A decision had to be made on how best to recover the aircraft back to home base. Two options were available, i.e. to fly in the defective condition with the system disabled or if not to call for a rectification team to the location where the aircraft had been stranded.

The need for risk assessment arose because of safety consideration, i.e. the consequences of an in-flight fire if the aircraft flew with a disabled system, and even the loss of an aircraft, but the judgment could have been clouded by commercial considerations, i.e. lost revenue, earning time plus cost of dispatching a recovery team.

This is a real life situation of a specific case where the flight crew, engineers and their managers would have to assess the risk and take a decision, based on evidence, their previous experience and knowledge of the system, and best subjective judgment. When costs are involved, and time is measured in terms of cost, an invisible business pressure is automatically placed on the specialists to take a decision quickly and to act upon it. A CEO might say that no one is putting commercial pressure on the specialists, but it is fact that specialists are aware that they would have to answer to the CEO or delegated authority, if their decision had a negative impact on the commercial aspect of the operation.

Either through correct rationalization or luck these decisions often end up with a positive outcome. Occasionally however decisions taken in haste due to commercial reasons could turn up to be drastically wrong with a tragic ending. Spanair Boeing MD-82 EC-HFP, Flight 5022, which crashed during takeoff at Madrid airport on the 20 August 2008 killing 154 of the 172 occupants is a case in point. See Appendix 2 for a brief outline of likely causal factors according to the interim investigation report[40].

3.10.2 Record keeping of decisions

Such, case by case risk assessment may be undertaken by engineers and managers in an organization many times as part of their mode of operation. Usually no records are kept on the way risk is assessed or what decision has been taken. The only information that could be seen is probably a record of the situation and the final action taken. Any intermediate records would be kept only if any other formal administrative actions had to be taken as a part of the management or decision process.

Ironically there is a dearth of management tools available to the specialists. Following industry best practices some organizations are known to have created and maintained decision flow diagrams or such diagnostic tools. In a report produced by Leach[15] on the aftermath of another investigation into a maintenance error induced flight incident, as reviewed in Section 4.2, he concedes that it is humanly impractical to provide this type of diagnostic and decision tools for thousands of different situations that could arise in a maintenance environment or any specific aircraft type.

3.11 Regulatory requirement

Employing risk management strategies to assist in the effective use of resources is one characteristic of an effective State controlled safety management system that is generally known as the regulatory framework. This is the recommended balanced approach to control and supervision of civil aviation industry according to ICAO Safety Management Manual[41]. Putting this recommendation into practice, safety risk assessment is undertaken by the Regulator as a part of the process leading to the initial issue of a Type Certificate, Airworthiness Certificate or an operating license that identifies a business entity as an approved organization. Risk is reviewed by the issuing authority whenever either these approvals fall due for periodic reviews, on license holder's request to make changes or during routine surveillance and safety audits of organization and its aircraft.

3.11.1 Aircraft - Risk at Type Certification and Airworthiness Certification

It was already stated that continuing airworthiness process starts from the time an aircraft enters operational service, first having registered the aircraft and obtained an Airworthiness Certificate, see Section 2.5 – 2.6. Having a valid Type Certificate is one pre-requisite for an Airworthiness Certificate.

The TC confirms that the aircraft has been designed produced and tested to exacting standards that is already laid down elsewhere in regulation, e.g. EASA CS-25, and that

the applicant organization has fully complied with the relevant regulation in accordance with EASA Part 21 DOA/ POA.

One set of information of particular interest to this research study is the design risk level of an aircraft that initially enters service. The regulations state[42, 43] that the probability of a catastrophic failure of the aircraft must not be worse than 1 x 10E-07 flight hours; this probability is qualitatively defined as extremely remote. The probability value is considered as a threshold design safety level for a civil transport aircraft, due to likely hazards from all systems collectively.

In practice it is not possible to determine if this target threshold has been achieved without numerically analyzing the effect of all systems together collectively. Therefore, the target rate has been equally apportioned amongst arbitrary 100 potential failure conditions that could lead to a catastrophic accident, each receiving risk rating of 1 x 10E-09 flight hours (extremely improbable)[42, 43] . Naturally, there could be conditions that would lead to less severe consequences and therefore a higher frequency of occurrence is admissible for them.

Usually the declared risk levels contain safety factors to cover threat to safety from unknown and imponderable conditions. A safety factor 3.33 is used if the result is based on testing, or factor 5 or more if on calculations[44]. Factor 3.33 is the linear scaling factor between the mean value of test results and a point that is 3-standard deviations to the left of the mean value in a log-normal probability distribution curve of a large number of test results; this point gives approximately 1 in 1,000 chance of a test failing in a series of similar tests that go to make up the distribution curve. The mean value is considered as the 50% chance of the test specimen failing at that test duration, measured in the log of the number of test cycles, which is equivalent to the probability of a component failing at the end of its service life that has no safety factor incorporated. By factoring down the test result, a safety factor is incorporated.

This method of setting the fatigue life of aircraft structural components is based on safe life design and a fatigue test. Confidence in the safe, factored-down life is further increased by monitoring the fatigue life usage in service, which incorporates the recording of loading cycles and magnitudes of loading encountered by the aircraft in service. Loads monitoring is intended to provide a comparison of the test loading conditions with in-service loading and thereby to account for significant deviations, if any.

If there is no specimen test, the calculated value is factored down by 3.33 similar to a test result; then to make up for unknowns about how a test specimen might have behaved under test, the result is further reduced by a factor 1.5; it gives the Factor 5 =

3.33 x 1.5, an acceptable level of confidence. In alternative damage tolerance design, safe inspection intervals, instead of safe life, are based on a calculation and Factor 5.

The current practice to determine the collective effects of all known critical hazards is to physically test the aircraft for static strength, for fatigue strength, as well as for reliability and durability under extreme environment conditions that the aircraft is expected to encounter during its operational life. Unfortunately, only one full scale aircraft is usually tested because of the high costs involved, but the test result is considered as a mean value. The underpinning proof of concept has been demonstrated by past experimental research work on specimen structural joints.

3.11.2 Organizations - Risk assessment during initial certification and/or licensing

When business entities who wish to participate in relevant aviation activities apply to the national Authority for licenses to operate, the Authority would ascertain the competency of the organizations to perform the intended activities in a safe manner according to the regulation in force (Section 2.4.5). In this process, the Authority would assess if the applicant organization constitutes a flight safety risk, or if they are capable of reducing risk level to as low as reasonably practicable (ALARP).

Risk assessment is usually done on the basis of evaluating the subject, be that an aircraft or an organization, against a list of criteria set by the Regulator in accordance with the relevant regulation. Some of the criteria might have minimum allowable threshold limits that the applicant should pass, and some criteria might be weighted according to their importance for safety. The Authority determines the method of assessment, for example through a paper study, followed by interviews with the applicant and final physical verification by physical on-site inspection of the evidence presented. The organization infrastructure and facilities would be subjected to an oversight inspection until the assessor is satisfied that the risk level is negligible.

If this verification process reveals any shortcomings relative to the expected standards, the surveyor will record the shortcoming as a Finding against the relevant criteria. He will convey this inform to the organization's Accountable Manager by raising appropriate documentation and interview. A Finding may be at Level 1 or Level 2, the former requiring urgent remedial measure, whereas the latter a less serious, but nevertheless requiring remedy within a reasonable period. The documentation on Findings will stipulate the timescale for remedial measures to be applied, as agreed between the organization and the surveyor.

On initial licensing, an applicant is expected to meet all the criteria specified by regulatory requirements. If there are any shortcomings, they would be given more time within an agreed timescale to remedy it, before a license could be issued. Final

decision is taken on the basis if the organization poses a risk to flight safety and if it can be passed as competent to operate safely.

3.11.3 Risk assessment at change of condition

Since the initial certification of an aircraft or licensing of an organization is conditional, any change of condition such as varying operational scenario deems to require a review of the risk. The regulation identifies important criteria that may have a high sensitivity on risk. Significant changes to these criteria would call for a reassessment of the risk. The onus for initiating a request for reassessment lay with the operator or organization responsible. The Regulator would apply the same methodology of evaluating criteria against a known standard. However, in this instance, the track record of the safety performance of the aircraft or the organization would be examined and taken into account before determining the risk. The standards applicable are based on the knowledge and experience of the assessors, the minimum levels of which are specified as part of their job specification[45].

3.11.4 Risk assessment at planned oversight inspections

Even if an approved organization had no reason to initiate a request, e.g., there was no change in condition, the Regulator could initiate an oversight inspection program as part of its surveillance and auditing of standards. This comes under one of the State's responsibilities[45] as previously described in Section 2.11.

ICAO guidelines recommend that all the relevant factors of an organization or an aircraft should be inspected in one 2-yr cycle. This periodicity may vary according to the historic safety performance of the organization or operator, subject to Authority's discretion. The surveyor responsible for oversight inspections would prepare an inspection schedule covering a period of 2-years, during which he would inspect the entire organization and its aircraft progressively, part by part, until the full 100% is completed during the inspection cycle.

The methodology for oversight inspection, assessment and decision making process is the same as before, i.e. by evaluating the organization and its change of conditions against a set of criteria defined by the Regulation. See Appendix 13 for a specimen EASA Part 145 Approval Surveillance Record of Findings.

A Finding, especially at Level 1, that has not been remedied within the agreed timescale could lead to a warning. A repeated failure to comply with the undertaking would lead to the revoking of the license to operate, that could affect the organization's trading position. Likewise, the airworthiness certificate of an aircraft could be revoked if it was found that no remedial action has been taken on a Finding

even after repeated warnings. In this case, the Approved Organization or the aircraft associated with the Finding is deemed unsafe.

3.11.5 Routine time-based review airworthiness certificates

To prevent unobserved deterioration of conditions of an aircraft's airworthiness, there is a requirement to review the Airworthiness Certificate at periodic intervals as per EASA Part M MA901, usually annually. If the review is satisfactory, then an Airworthiness Review Certificate (ARC) is issued either by a Continuing Airworthiness Management Organization (CAMO) or the Authority. If the aircraft has been operating in a controlled continuing airworthiness environment a CAMO could issue an ARC at 2-consecutive years, but on the 3rd year, the review would have to be undertaken by the Authority. If the aircraft had been operating in a non-controlled environment, the CAMO could undertake the review but only recommend to the Authority that an ARC could be issued. The Authority would then issue the ARC. If not the review could be done by the Authority itself and if satisfied, the ARC may be issued. In all these circumstances, implicit with the review is a risk assessment process, but it is effected by evaluating the aircraft against the criteria set by the regulation.

3.12 Risk assessment as part of strategic planning and resourcing

Independent from the regulatory processes and tactical planning under operational conditions, risk assessment may be undertaken as part of an organization's strategic planning. This type of assessment may be done as part of setting up a safety management system, or if an SMS is already in position, then as a part of a long term program under SMS to improve the organizations safety profile. For example, a CEO might decide that there ought to be a vigorous campaign to reduce incidents by 20% over a 12-month period. A good starting point is to draw up a baseline of risk contribution from each department of his organization, and to use this as a reference line from which progress could be monitored. The reference line could be extended to cover important, high profile processes within an organization where accidents are known to happen, or for groups of employees that are more prone to accidents than others. Reduction of accidents due to human error falls into this category of risk assessment for strategic planning.

3.13 SMM guidelines on risk assessment methodology

On the method of risk assessment, Safety Management Manual (SMM)[38] provides guidance. According to SMM, an organization and its operation should be analyzed to:

a. Determine unsafe situations or conditions that could lead to accidents (usually fatal or catastrophic).
b. Identify hazards associated with the unsafe situation.
c. Assess risk.
d. Mitigate and reduce the risk, and finally
e. Communicate findings to all concerned.

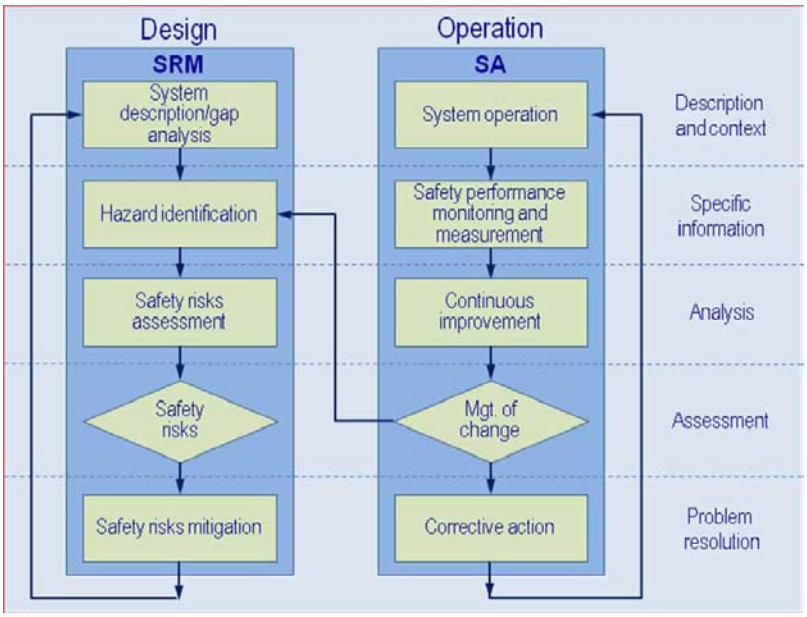


Figure 3.2 - Safety risk management process
(Source: ICAO Doc 9859 2nd Ed)

Figure 3.2 demonstrates the flow diagram of activities covering safety risk management as part of the SMS design (i.e. planning phase) followed by SMS operation where safety is assured. Risk assessment is part of the planning phase. Assessment of risk requires prior knowledge of the probability of the hazard precipitating an unsafe event, and the severity of the adverse consequence. This is in fact represented in the formula:

$$R_{total} = \sum_{i=1}^{n} L_i \,.\, p\,(L_i) \qquad 3.3$$

3.14 Severity of consequences and probability of occurrence

Traditionally the types of consequences and their severity have been defined qualitatively, based on experience. Probability of consequence of a given severity arising is also expressed qualitatively, mainly because of lack of sufficient hard

evidence. If a numereical outpt from risk assessment is required, the qualitative definitions of severity of consequences could be converted to a numerical liner scale as presented in Table 3.2. The way cost of accidents escalate, it is debatable if this type of linear scaling is valid or not.

Current definitions of consequences have evolved as a result of observing accidents and contributory conditions, i.e. hazards. However when assessing a situation that could end up with an accident, where evidence may not be glaringly obvious, an assessor may find it diffcult to allocate a likely consequence. Guidance from ICAO definition of risk is to consider the outcome of a worst foreseeable situation given the hazard exists; it is common knowledge in civil aviation industry, that the interpretation of this definition is difficult and if people always go strictly by the book in practical situations then nothing would get done.

Severity of Consequence			
Aviation definition	**Meaning**	**Alpha-numeric value**	
Catastrophic	Equipment destroyed. Multiple deaths.	5	A
Hazardous	A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely. Serious injury or death to a number of people. Major equipment damage.	4	B
Major	A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of an increase in workload, or as a result of conditions impairing their efficiency. Serious incident. Injury to persons.	3	C
Minor	Nuisance. Operating limitations. Use of emergency procedures. Minor incident.	2	D
Negligible	Little consequence.	1	E

Table 3.2 - Severity of consequences – Definitions (Source: ICAO SMM)

For example, if a fuselage panel of a pressurized aircraft has a large fracture line running along it, one would not release that aircraft to fly. If it flew, the consequences could be catastrophic. However if an airfield manager had to delay the runway sweeping by few hours to allow a training exercise to take place, thereby missing a routine sweep, how would he judge the potential consequence and risk. In this latter case the whole range of consequences may be valid, or equally possible. In the case of Air France Concorde accident, the manager of the airport had opted to delay the runway sweep probably assuming no significant consequence and low risk. But the actual outcome was the loss of a Concorde with 109 occupants[9] aboard, that might have partially contributed to the decision to retire the Concorde fleet, see Appendix 2.

In most situations encountered in real life, more than one consequence may be possible. The specialist may have to select one, and it is likely that he would be

swayed by fear and uncertainty as well as self protection, whereas the managers who are responsible for the revenue generation and commercial utilization of aircraft may urge the specialist to dilute his judgment on the grounds of uncertainty and business objectives. Whilst there is some leeway to discuss and compromise at times of strategic and planning situation, there is little time at tactical situations when a urgent decision has to be taken in the face of various odds.

3.14.1 Applying subjective judgment under stressful conditions

It was mentioned by one CEO that commented on the study, that businesses never apply pressure on flight crew when to take off or where to land if there are adverse conditions, as it is the captain who decides and voluntarily takes the risk. Factually that may be correct on the basis of the terms of reference for a captain, but it is at best naive to pretend to ignore the captain's relationship to the purpose for which the aircraft is flown. If the aircraft is lost due to a wrong decision, the psychology behind a captain's decision and action is invariably lost with his death and investigators end up with having to determine if a flight crew was put under pressure or not. The recent loss of the Polish Air Force TU-154 carrying the Polish President on 10 April 2010 vividly demonstrated this phenomenon as reported in the media the possibility of the captain coming under pressure from his political superiors onboard[46].

It is quite normal to experience a certain amount of stress in every business organization, and occasionally to exceed it beyond the norm. Whilst that may be a reasonable starting point, this study was receiving information that norms are occasionally stretched beyond tolerable levels, as business managers sweep out reason in the name of cost savings and business expediency. When it comes to safety, one has to remember that safety does not come at no cost and, therefore, the cost threshold used in exercising ALARP philosophy remains a moot point .

Discussions with some members of the Association of Licensed Aircraft Engineers (ALAE) have alerted this research study that engineers who are at the sharp end of delivering an airworthy aircraft for flight are under constant business pressures thrust upon them. Ironically they are often the very last but one defence against errors that the continuing airworthiness process might have carried forward. Existence of such pressures are substantiated by various related reports received by CHIRP, an organization set up to receive confidential reports from aviation industry[47] .

Although the foregoing commentary appears be a diversion from the topic in hand, it is related here in order to demonstrate the difficulties and uncertainties of applying a subjective judgment on the potential consequences when considering safety cases.

Also, it is debatable if someone is mentally capable of assimilating all hundreds or even thousands of combinations of diferent situations rationally, and then to take a judgment on how frequently it could happen. It is no better than making a statement or a prediction about something that cannot be verified in one's lifetime, because there is no way that sufficient evidence could be gathered to prove or disprove the prediction or estimate. Despite this severe limitation, this type of qualitative definition is used in risk assessment.

Table 3.3 presents the categorization and frequencies converted to a linear numeric scale. Alongside the numeric values, the Table presents the EASA CS -25 definitions of the probabilities converted to numeric values.

Likelihood of Occurrence			
Qualitative definition	**Meaning**	**Numeric value**	**EASA CS -25 rating Failure probability per FH**
Extremely improbable	Almost inconceivable that the event will occur	1	10E-9
Improbable	Very unlikely to occur	2	10E-7
Remote	Unlikely, but possible to occur	3	10E-5
Occasional	Likely to occur sometimes	4	10E-3
Frequent	Likely to occur many times	5	10E-2

Table 3.3 - Probability of occurrence of consequences - Definition

3.15 Rate of exposure

SMM also introduces another variable, namely the rate of exposure to the hazard. This term in fact needs a closer scrutiny. If $p\ (L_i)$ is the general probability of a certain type of consequence occurring, say at global level, then the rate of exposure is related to a specific organization which might have an exposure rate to the same potential consequence that may be at a higher or lower than the global rate. For example, assume that the global rate of accidents during short runway takeoffs is 10 per year. However if an airline has a home base with only a short runway, and all its outbound flights have to takeoff from this airport and all inbound flights have to land there, then the exposure rate to the hazards of a short runway may be higher than that for the flights considered under global case. That means, exposure rate depends upon the size of the population considered, which encounters a specific hazard from which the frequency of exposure has to be determined. It is an important parameter to be used when interpreting a result of risk analysis, and in determining how confident one could be in using the result.

3.16 Data availability

The scarcity of data may dictate the risk assessment methodology. Civil aviation is already operating to a very high level of safety despite the occasional catastrophic accident. This means that there is a dearth of data in different combinations of "conditions-consequences", i.e. the number of potential combinations may run into millions, whereas the number of accidents and recorded conditions may be relatively small. Recognizing this impasse, paragraph 6.3.4 of SMM[38] (First Edition) states:

"There are many ways – some more formal than others – to approach the analytical aspects of risk assessment. For some risks, the number of variables and the availability of both suitable data and mathematical models may lead to credible results with quantitative methods (requiring mathematical analysis of specific data). However, few hazards in aviation lend themselves to credible analysis solely through numerical methods. Typically, these analyses are supplemented qualitatively through critical and logical analysis of the known facts and their relationships."

The most widely known and universally accepted risk assessment model is based on this principle of mixing qualitative definitions converted to a numerical scale: this gives a 2-dimensional matrix, on one axis the likelihood of occurrence ranked along frequency, and on the other axis, the types of consequences ranked in levels of severity.

3.17 Traditional risk matrix

Table 3.4 presents a traditional risk matrix used for assessing risk in civil aviation.

Risk probability		Risk severity				
		Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E

Table 3.4 - Safety risk assessment matrix (Source: ICAO Doc 9859 2nd Ed)

The variables on the 2-axes have been graded by a either a numerical value or a letter that simply defines its hierarchical order, and NOT because they have a mathematical or a physical relationship. For example, a consequence considered to occur at a very low frequency and allocated a value 2 is not physically related to another one, e.g., a frequent event that has been allocated a value 5, by a factor 2.5. The numbers simply

signify their importance. A catastrophic accident might cost 300 lives and an insurance claim of £1 billion, whereas a minor accident might result in relatively benign injuries and damage to assets of the order of £5,000. CAP 642 Airside Safety Management[48] offers some examples of the way this type of risk matrix is used.

The closer analysis of the matrix might be seen as trivial, but it is an important point in determining how good the matrix is for assessing risk, and if the output truly represents prevailing risk.

Nevertheless, using the simple formula a linear risk scale has emerged from this matrix.

$$R = \text{Probability of consequence} \times \text{Severity} \qquad 3.4$$

The most important feature of the matrix is its capability to represent risk level graphically, which allows the user of the model to gain a sense of proportion qualitatively rather than as a physical value to it. The convention, practiced by successive generations of assessors, determines if the risk level is acceptable or not, but this depends very much on the experience and subjective judgment of the assessor (best described as his feel) rather than on evidence of sufficient outcomes.

Table 3.5 represents the assessor's thinking on what combination of severity of consequences and probability of occurrence could be acceptable, be rejected and if uncertain could be negotiated or rationalized before a decision is taken. These are subjective, because in this system, even with prior definitions of categories, interpretation of the thresholds could be subjective, and variable between different assessors. In the circumstances to the Air France Concorde accident[9] a tolerable 3B level risk index turned up to be a 3A, demonstrating that conditionally other factors could come into play , despite they were beyond the assessor's imagination.

It may be possible to reduce this uncertainty of thresholds by placing true values for the severity of consequences, and by substituting true, numeric probability values.

Risk management	Assessment risk index	Suggested criteria
Intolerable region	**5A, 5B, 5C, 4A, 4B, 3A**	Unacceptable under the existing circumstances
Tolerable region	**5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D,2A, 2B, 2C**	Acceptable based on risk mitigation. It might require management decision
Acceptable region	**3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E**	Acceptable

Table 3.5 - Safety risk tolerability matrix (source: ICAO SMM Doc 9859 2nd Ed)

Table 3.6 was generated by this study to present risk as a financial risk, where the severity of consequence is represented as a monetary value. The probabilities used are numerical values extracted from EASA CS-25 definitions for Design Requirements of civil aircraft. Discriminating between risks, i.e. acceptable, unacceptable, and acceptable after mitigation is much clearer here as it is backed by a quantitative parameter that is more meaningful than a just a number, in this case financial risk per flight hour against a possible maximum cost if accident did take place.

Severity of Consequence	Cost of accident (£)	Risk (monetary value)				
Catastrophic	10E9	1	100	10000	1000000	10000000
		0.1	10	1000	100000	1000000
Hazardous	10E7	0.01	1	100	10000	100000
		0.001	0.1	10	1000	10000
Major	10E5	0.0001	0.01	1	100	1000
		0.00001	0.001	0.1	10	100
Minor	10E4	0.000001	0.0001	0.01	1	10
		0.0000001	0.00001	0.001	0.1	1
Negligible	10E3	0.00000001	0.000001	0.0001	0.01	0.1
	Events per hour	10E-9	10E-7	10E-5	10E-3	10E-2
Probability of Occurrence		Extremely Improbable	Improbable	Remote	Occasional	Frequent

Table 3.6 – Risk matrix presented in monetary terms

In this matrix the cost bands do not have any known previous precedent but a range estimated by the researcher to demonstrate the concept of a risk matrix based on cost. For example, an upper limit of £1B was set against catastrophic accidents. This figure was based on figure of £600M estimated by a panel of lawyers and underwriters as the full cost of settling claims, in a simulated damage assessment exercise relating to a fatal accident to an aircraft of the Boeing 737 class. It was assumed that the aircraft was totally destroyed and all occupants died[49]. The costs included payments to victims, liabilities to the operators and manufacturers, cost of investigations and all round legal fees. There were no victims on the ground.

£1B is not necessarily the upper limit of this Band, as it could be extended according to the type of aircraft, number of victims and the extent of claims due to both direct and collateral damage, and what a court may set.

The £100M lower limit represents a change over point from the upper limit of a hazardous accident where there were no fatalities, and the hull might be salvaged.

Thus, £100M to £1B may be a reasonable range for a typical aircraft accident at the 2008 economic conditions.

Once the uppermost band was set, the lower bands were scaled down using a log scale putting the limit of minor costs around £1,000. This is roughly the cost of handling a reported error incident, involving one-week of work for an investigator. Any smaller costs may be negligible.

3.18 Extent of usage of traditional risk matrix

The extent of usage of the traditional risk matrix within the civil aviation industry is not clear. Over a period of 3-years this research study observed opinions expressed by subject experts attending routine, national level flight safety meetings at which nation-wide air operators and maintenance providers were represented. Everyone was aware of the guidance on the use of risk matrix, and many have used it occasionally to assess risk at specific situation involving identified safety cases. However there was no uniformity of its use and certainly as SMM guidance is advisory, approved organizations applied the technique on an ad-hoc basis. Considering the industry as a whole, use of the risk matrix is widely known, but the number of occasions that it is used by any one approved organization may be very few.

Part of the difficulty in the use of risk matrix is the dearth of data that is necessary to substantiate intermediate decisions, such as the probability of occurrence of hazards not previously encountered.

3.19 Data gathering practices in industry

Given these limitations on risk assessment, industry-wide, much effort in risk management activities is spent on data gathering, categorization and analyzing trends. This is done under error reporting and investigation process that has been formalized by regulation and in UK promulgated by UK CAA under CAP 382 Mandatory Occurrence Reporting System (MOR)[50] and under CAP 562 Leaflet 11-50[51] (formerly UK CAA Airworthiness Notice 71 on Maintenance Error Management System (MEMS)[52]. These together with other air and ground incidents contribute to error data banks that help to understand trends, and correlation between errors, consequences and their causal factors.

3.19.1 Incident reports

Air and ground incidence reports relating to maintenance error, or human error at design, production and integrated logistic support planning and implementation were

of interest to this study. Equipment shortcomings and their unreliability due to limitations of design, production and testing standards were not within the scope of this study. Some of the reports are described below.

3.19.2 Mandatory Occurrence Reports (MOR)

Incidents that damage an aircraft or injure a passenger, or have potential airworthiness or safety implications are reportable to the National Airworthiness Authority under the CAP 382 Mandatory Occurrence Reporting system. Air operators usually retained detailed results of their investigation, and a summary report is forwarded to the Regulator. Reports sent to UK CAA are retained under confidentiality agreement.

CAA Paper 2007/04 Aircraft Maintenance Incident Analysis[53] which examined about 3000 MOR reports sent over a period of 10-years, had reported that very little details of company investigations had been reported in MOR submissions.

Given that MOR route was going to be unsuccessful in determining causal chains, attention shifted to the possible use of approved organizations' proprietary data, retained by them under the Maintenance Error Management System.

3.19.3 Maintenance Error Management System (MEMS)

MEMS were initially brought into use under UK CAA Airworthiness Notice 71 (2000)[52], now Leaflet 11-50 of CAP 562[51], as part of the Human Factors education and promotion programme, the purpose of which was to prevent the recurrence of maintenance error. The concept behind MEMS is that it is prudent to catch and eliminate errors that lay at the bottom of the "error-iceberg" as early as possible in order to eliminate the possibility of their becoming serious problems later on.

Approved organizations are expected to report, record and investigate maintenance error, and to take follow up action to prevent the recurrence of similar errors. Demonstration of compliance with CAP 562 Leaflet 11-50 is currently part of the routine Regulator's oversight inspections.

Usually MEMS is managed by the organization's Safety and Quality Department. Under good safety culture, personnel are encouraged to report error incidences without the fear of being victimised for their voluntary action.

This is part of the progressive campaign within an organization to minimise human error related incidents. Incidences are dealt with within the organization, investigated and records are retained in a databank. Usually reported incidents are investigated using MEDA format as the route map for analysis, and medium of communication.

3.19.4 Maintenance Error Decision Aid (MEDA)

MEDA stands for Maintenance Error Decision Aid, a management tool in the style of a formatted document (when completed) that could be used to record details about the error incident. Its completion is done by a trained investigator, concurrently with the investigation, in which the reporter assists by way of a dialogue with the investigator.

MEDA taxonomy has been initially designed, developed and recommended to the global aviation industry by Boeing Aircraft Company, and was initially published in a paper by Rankin (2000)[54]. At present MEDA had been accepted as an investigation and classification tool to determine causal factors of an error incident, and an input tool to a larger MEMS database. The error type and causal factor taxonomy used in MEDA is fairly comprehensive, but as more and more experience is gained, there have been gradual improvements to the MEDA form. MEDA Form Issue H is the current version, but continuation improvements are on-going.

A User Guide to MEDA could be obtained from Boeing (2010)[55]. As for MEDA applications, an overview of a maintenance error management system by BF Goodrich using MEDA has been described by Bongard (2001)[56].

3.19.5 Company proprietary databases

It is known that some approved organizations maintain company proprietary data bases using commercially available, web-based software tools. Vistair's Safety Net[57] and AQD Superstructure Group's Integrated Safety and Risk Management[58] are two typical packages, both web-based. The respective commercial organizations maintain the database and facilities, and air operators or maintenance organizations could become users by purchasing an on-line access to use their system.

Most of the web-based databases generally available to civil aviation industry are principally depositories for incident reports, MEMS reports and any other similar data. They provide facilities for categorization and analysis of trends, but do not go as far as applying these data to determine the risk for the organization or flight safety. That

aspect remains the prerogative of the assessors that would use the data from the database.

AQD for instance claims that it offers*, "tools for creating internal audit programs, assisting with audits for all departments, tracking corrective and preventive actions, integrating external audit requirements and analyzing and reporting trends in quality indicators".*

AQD Software in contrast to most others offer a facility for recording results of risk analysis process, i.e. identifying hazards, potential consequences, and available evidence from which probabilities could be determined, against each safety case. It also has facilities to register risk level before and after a risk is mitigated. However the mechanism for analysis is subjective and left to the assessor, outside the software package. AQD software does not have a module for risk assessment.

3.20 Analysis of Data

3.20.1 MOR data

UK CAA collects MOR data under commercial confidentiality, and along with accident data they may be of benefit to UK CAA as indicators of the general state of safety within the industry. For the benefit of participants, UK CAA produces a monthly list of MOR submissions, giving essential data and a brief narrative of events. On request, CAA provides ad-hoc reports and analysis of dis-identified data back to participants of the scheme. MOR data are not used for assessing risk either at individual organizations or industry as a whole.

Using MOR data collected over 10-years, CAP Paper 2007/04[53] reported on the incidence of human error in maintenance. There had been 2924 low risk maintenance errors and 21 high risk errors during the period studied. A large proportion of MOR was attributed to role equipment and furnishings (19.2% of the low risk errors and 9.5% of high risk errors). However on high risk errors, combination of propulsion related systems (15.0% low risk, 23.8% high risk) and landing gear (11.0% low, 23.8% high) were leading with flight controls ranking third (9% low, 19.0% high) respectively. CAP 2007/204 made no attempt to assess the level of risk in industry using MOR data.

3.20.2 CHIRP/MEMS

CHIRP is an acronym for Confidential Human Factors Incident Reporting Programme. It has been set up to receive confidential reports from those involved in aviation activities, who feel that they are unable to report incidents under the existing MOR

scheme for fear of pressures and intimidation from their superiors or peers. It is however complementary to MOR scheme, and data is analyzed and fed back into the main system first having investigated the matter and ensured that the identity of the originator has been removed. CHIRP has been established as a charitable company, ensuring that the confidentiality of the information it receives is legally protected[47].

Since the original formation of CHIRP, its activities have been extended. Now there is much more open discussion between CHIRP and civil aviation industry as a whole. Within CHIRP is the UK-MEMS Group, composed of 25 member organizations with interest in air operations, maintenance, training and defence, which regularly meets every 2-month to discuss issues and share information pertinent to flight safety and error management. While still receiving confidential reports as originally intended, CHIRP MEMS now receive both MEMS data directly from industry and MOR data from UK CAA. These are desensitized and analyzed, and outputs are published in the CHIRP/MEMS web-site [47] as well as desensitized narratives of confidential reports and investigations.

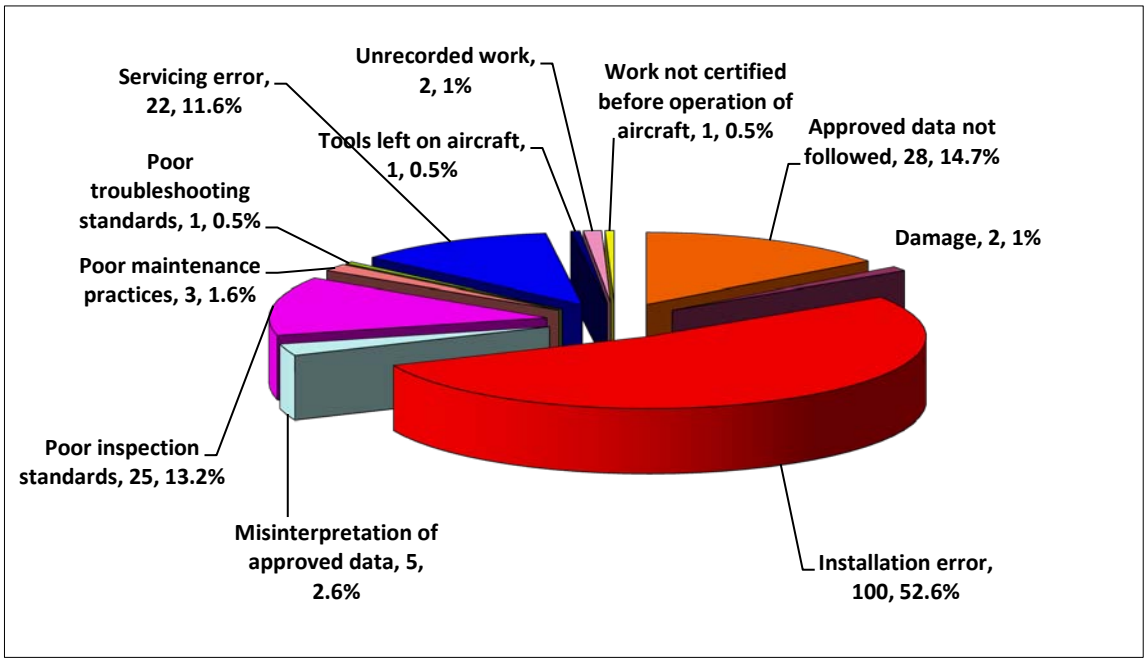


Figure 3.3 – Sample 1 of MOR/MEMS data analysis published by CHIRP
(Source: CHIRP/MEMS) Number of hits and percentages rounded to nearest decimal place

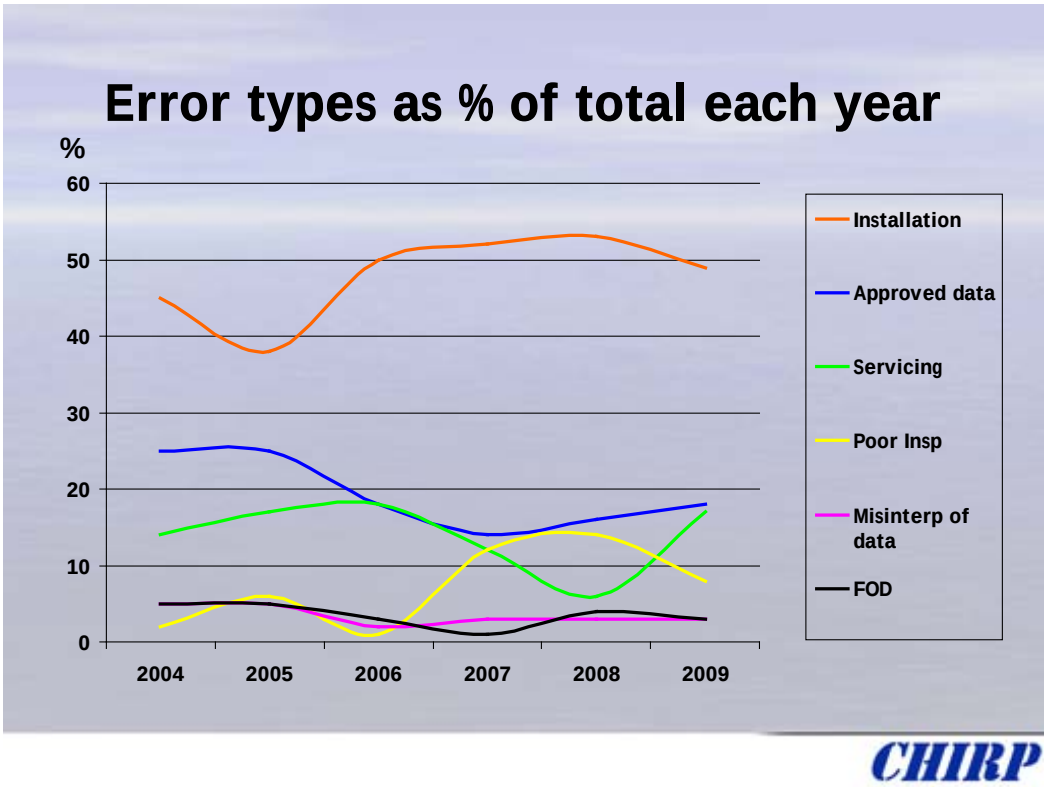


Figure 3.4 – Sample 2 of MOR/MEMS data analysis published by CHIRP
(Source: CHIRP/MEMS)

As with many other database systems, CHIRP MEMS is still a depository for data. Analysis is limited that they are confined to designing different taxonomies and trend analysis. Trend analysis is important because it provides relationships between types of errors and their causal factors, as well as if the occurrence rates are increasing or decreasing. However when faced with multiple types of errors and multiple causal factors interacting within the same process system, a manager would like to know their net effect as an overall risk to the end product, and its sensitivity to contributing errors. That way, the manager would gain a better comprehension of the significance of errors and the knowledge and confidence to control them in an order of priority. Although MEMS are interested in a means of pulling together all available MEMS data to provide an industry wide risk assessment methodology, it has yet to be realized.

3.21 Other countries

As part of this research study, methodologies adopted by two other foreign regulators, US Federal Aviation Agency and Civil Aviation Authority of the Netherlands (NL-CAA) were briefly studied. Both countries had put in place very similar practices to those employed by UK CAA in initial licensing of approved organizations, and subsequent regulatory oversight inspections, as well as determining priorities

regarding the organizations that needed more attention. However in the more recent times both Regulators have adopted more cost-effective methods. For example, FAA has opted for a system called Safety Performance Analysis System (SPAS), whereas NL -CAA has introduced a more sophisticated method based on Multi Criteria Decision Analysis.

3.22 Safety Performance Analysis System (SPAS) of the US

SPAS is an IT management tool developed for FAA by US Department of Transport's Volpe Research Centre, in collaboration with Computer Sciences Corporation[59]. It is a highly complex system of risk assessment program that feeds on several hundred parametric data lines on specific aircraft, engines, organizations and personnel, held in almost 40 separate State owned databases[60].

SPAS program enable its operators to access such data and then integrate and synthesize them according to predetermined subroutines that could be called up as required. All personnel involved in oversight activities in FAA (i.e. all at Flight Standards Services (FSS) who are equivalent to UK CAA SRG surveyors) are required to utilize this management aid, to integrate and analyze critical safety information available to them so that they could quickly identify risks and focus on inspection resources on areas of greatest priority [61].

The inception of SPAS that initially cost US$35M can be traced back to 1991. The system was fully operational by 1995. Despite high level of investment, SPAS has had its problems with data quality and integrity, but through further development and remedial measures they have been overcome and SPAS is continuing in service. Since SPAS is a secure system available to FAA and Department of Defense, information on software and algorithms are not available to public.

3.23 Risk assessment method by CAA of the Netherlands (NL-CAA)

Civil Aviation Authority of the Netherlands currently use a risk assessment model based on the concept of Multi Criteria Decision Analysis (MCDA)[62]. Here each approved organization is assessed against each of 3 broad areas, namely, Organizational Risks and Quality Risks, the latter encompassing both Regulatory requirements and Quality requirements focussed on the tasks. The model follows a fishbone architecture, identifying numerous parameters (or criteria) assessed by oversight inspectors. Evaluation of each organization against the criteria is done objectively since criteria have been well defined. However, the definitions are

qualitative. Built into the evaluation part of the software is a means of providing numerical scoring. The final output is a numerical value of risk that can be used to compare one organization with another.

The model is used to prioritize approved organizations according to risk level they posed, and to manage NL-CAA inspector resources. The methodology is effective and has been well recognized by airworthiness authorities and civil aviation industry. It serves the purpose of managing resources according to risk based oversight concept. However one weakness is that the risk obtained this way is not a true risk based on actual number of errors or failures, but an assessor's sense of risk or subjective judgment. The numbers simply convert the judgment to a numerical value.

3.24 Taxonomy research

Taxonomy is the structured way that human errors, their consequences and causal factors are broken down and categorised, and usually organized into a hierarchical order. Taxonomy research in human error management is driven by the idea that, if causal factors were identified and prioritized, then it would help determine where investments ought to be made for their elimination most cost-effectively. Since this area has been much researched and several projects are on-going in different countries, this study will not digress into that arena. Suffice it to say that there are several reputed taxonomies in current use; the well known are the Human Factors Analysis and Classification System (HFACS) and Maintenance Error Decision Aid (MEDA). MEDA was described in Section 3.21.4.

Quite often individual research groups tend to design their own taxonomy to suit local conditions, which makes it impossible to amalgamate results from 2 groups into one without reanalyzing at least one of the groups' data. The need for an international standard for HF taxonomy is essential if good progress is to be made into human error research. EASA will use ADREP 2000 standard, see Section 3.26.3.

3.24.1 HFACS

Human Factors Analysis and Classification System (HFACS) is the most widely known system of taxonomy. It has been developed by 2 behavioural scientists of the US Navy, Dr Wiegmann and Dr Shappell based on Dr James Reason's Swiss Cheese Model of accident causation. Shappell and Wiegmann (2000)[63] provide details of the HFACS system, which has been originally developed for the US Air Force and since then much widely used in civil and military aviation . HFACS is based on Reason Model and

focuses on the “holes” of the Swiss Cheese Model to understand their types, groupings and patterns of behaviour in their contribution to accidents.

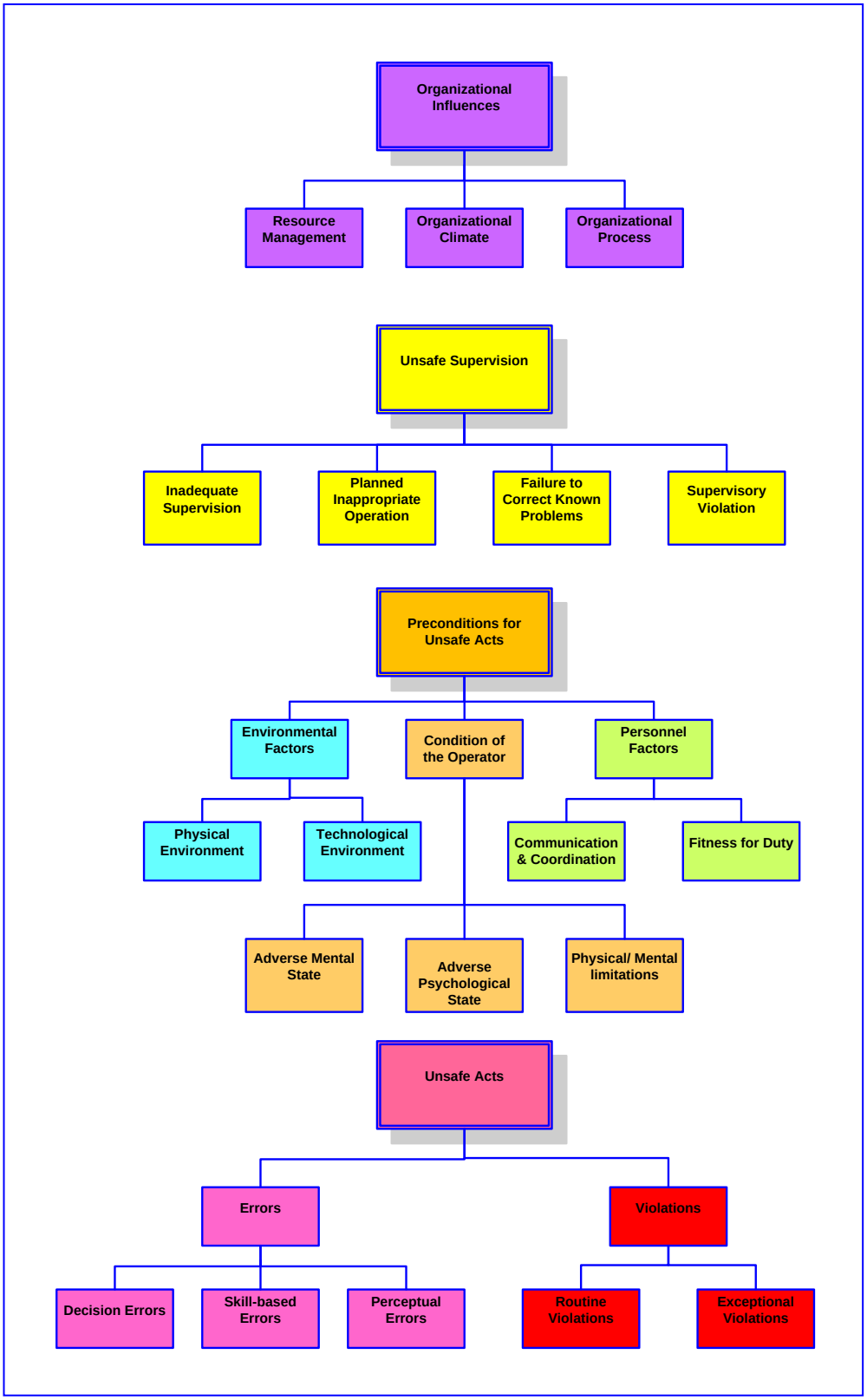


Figure 3.5 - The HFACS framework (Source: Weigmann & Shappell)

Figure 3.5 represents the basic HFACS framework they have developed. Using the framework as a guide, safety engineers and accident investigators can systematically identify and classify actual or potential failure causes in a human in the loop system. The objective of HFACS is to identify the causations of error and avert accidents through prior planning of defence mechanism, and not to blame any individual. However, HFACS does not provide and integrating mechanism to calculate the risk levels. HFACS has been designed principally for flight operations, but there is an airworthiness subset published by US Naval Safety Centre, a Student Guide sponsored by Watson and Kanki (2000)[64]. This maintenance engineering extension has the acronym HFACS (ME). HFACS (ME) categorization of human error in maintenance is given in Table 3.7.

First Order	Second Order	Third Order
Management Conditions	Organizational	Inappropriate Processes Inadequate Documentation Inadequate Design Inadequate Resources
	Supervisory	Inadequate Supervision Inappropriate Operations Uncorrected Problem Supervisory Misconduct
Maintainer Conditions	Medical	Adverse Mental State Adverse Physical State Physical/Mental Limitation
	Crew Coordination	Inadequate Communication Inadequate Assertiveness Inadequate Adapt/Flexibility
	Readiness	Training/Preparation Certification/Qualification Infringement
Working Conditions	Environment	Inadequate Lighting/Light Unsafe Weather/Exposure Unsafe Environmental Hazards
	Equipment	Damaged/Unserviceable Unavailable/Inappropriate Dated/Uncertified
	Workspace	Confining Obstructed Inaccessible
Maintainer Acts	Error	Attention/Memory Knowledge/Rule Based Skill/Technique Based Judgment/Decision-making
	Violation	Routine Infraction Exceptional Flagrant

Table 3.7 - Error categories of HFACS-ME framework

3.24.2 HILAS

Human Integration into the Lifecycle of Aviation Systems (HILAS) is a European Commission funded international research project based at Dublin University, Ireland. About 40 partners from aviation industry and academic institutes across European Union and beyond are collaborating in the project.

HILAS internet website states the objective of the project, which is *"to develop a model of good practice for the integration of human factors across the full-life cycle of aviation systems"*. Four parallel lines of research have been planned:

- Integration and management of human factors knowledge.
- Flight operations and environment and performance.
- Evaluation of new flight deck technologies.
- Monitoring and assessment of maintenance operations.

The last line of research is of relevance to this study. It is understood that part of the research relating to maintenance operating is geared to setting up common human factors taxonomy.

3.24.3 ECCAIRS

ECCAIRS is an acronym for European Co-ordination Centre for Aircraft Incident Reporting System. It is an EASA initiative for the collection, analysis, dissemination and storage of data from civil transport aircraft registered in or operated by European Union countries; as such all EC countries are participants to the ECCAIRS programme. ECCAIRS is operated by an EASA organization based in Italy and further information could be found on the EASA website[65]. ECCAIRS implements ICAO ADREP 2000[66] taxonomy and input data would have to be that standard[65].

Despite participation by all EU countries, in practice their actual data contributions have not been strong nor consistent due to various national issues, some political or commercial and others technical, such as differences in taxonomies used.

This research study has investigated the possibility of using ECCAIRS data, although it was known that ADREP 2000 taxonomy is more focussed on flight operation aspects of an accident rather than CAW matters. Unfortunately it was established that, at the time, insufficient progress had been made to supply and uptake UK civil aviation incident data, in the form of converted MOR data. It was understood that other data in ECCAIRS database, which France and Germany had already supplied to ECCAIRS,

were not relevant to commercial fleets. Thus EASA/ECCAIRS was unable to assist this research program with relevant data.

3.25 Risk posed by aircraft to population near airports

Hale (2000)[67] has studied the risk posed by aircraft to people living close to busy airports in the context of the El Al cargo aircraft accident in the vicinity of Schipol aircraft (see Appendix 2)[24]. Cargo aircraft consider to be posing a significant risk because they are usually relatively aged aircraft of average age of 28-years relative to the average age of 7-years for passenger aircraft. Passenger aircraft too pose a similar threat because the number of passenger flights is more numerous compared to cargo flights. In a study of risk to airworthiness, older cargo aircraft draw special attention even though in this study cargo aircraft are considered in the same context as passenger aircraft regarding their operating to international safety regulation.

That said, in the context of aircraft operations, risk to conurbations of population is considered as a third party risk. Ale (2002)[68] defines three key factors that affect third party risk: the individual risk, the societal risk and the risk of potentially losing life in a given year. To combine this with living close to an airport, other factors have to be taken into account. According to a methodology developed by the Netherland's National Aerospace Laboratory (NLR) (Ale et al 2000)[69], the probability of an aircraft crashing in the environment close to an airport is influenced by:

- Probability of an accident per aircraft movement, i.e. either a landing or a takeoff.

- Volume of airport traffic, i.e. aircraft movements, per year.

- Accident location probability, i.e. the probability of a given location becoming a scene of accident. This depends on its position in relation to the runway and aircraft flight paths.

- Accident effect model, which combines the effects of probability of an accident at each location in the area surrounding the airport. Accident effect takes into account the type and characteristics of the aircraft, the material carried in it, the size and terrain of the accident location.

Combined with this calculation are the individual risk factors that determines the probability of an individual living close to an airport, societal risk factors such as the density of population in the likely location of accident, and timing of the accident.

Finally, before leaving this area of investigation into risk to the people on the ground, it should be stated that the UK has a policy of public safety zones (PSZ) in areas surrounding airports beneath the flight paths, especially those aligned with the runways. The risk levels are defined by risk contour-lines that define the probability of a single fatality per year due to an aircraft movement. The established tolerable risk, or threshold, is defined as a probability of a fatality of 10E-04 per year; if the probability exceeds this value then the risk is considered to be unacceptable. Habitation and new buildings are not permitted within the area covered by the threshold risk contour. This criterion is consistent with the tolerable risk from other high risk industrial installations such as nuclear or chemical plants[69].

It is interesting to note that the tolerable threshold risk level for population, as accepted by civil authority, is much higher than the design risk level of catastrophic failure for civil aircraft of 1 in 10E07 flight hours (see Section 3.13.1). Obviously, a question follows from there: to what extent human error in continuing airworthiness might be undermining the design risk level of an aircraft?

3.26 Aircraft's contribution to the level of risk at ground

It was stated in the previous section that the type and role of the aircraft and its characteristics influenced the calculation of risk to the population living in the surrounding area of an airport. But there was no mention in the cited references the significance of the state of airworthiness of the aircraft. Therefore the presumption seems to be that if an aircraft has been certified as fit to fly, then it must have been airworthy according to regulation.

As to the reasons why aircraft have accidents near airports or anywhere else, suffice it to mention here that one reason is an airworthiness issue, despite that the aircraft has been certified as continuingly airworthy. Despite the fact that the aircraft has been released to service according to the regulation, yet it could be carrying an incipient, dormant hazard in the form of a human error or a mechanical unreliability such as a structural fatigue crack that manifested itself during the flight. That puts the onus on the aircraft operator to ensure that the aircraft's continuing airworthiness is maintained as required by regulation, and that human error does not undermine its airworthiness. This study is of course addressing the capability to assess the risk from human error in continuing airworthiness process that might help to mitigate the risk.

Other causal factors for accidents are attributed to flight operations, air traffic control, air field conditions, some of which are associated with human error in those operations. Moreover, there are other natural hazards in the vicinity of airports that

cause accidents such as freak local weather conditions, bird strikes and lightning strikes. These are topics outside the scope of this research thesis.

Amongst the factors that Roelen et al (2000)[23] have identified as contributing to cargo aircraft accidents are:

- Night flying.
- Operating in extreme cold weather, particularly in North America.
- Flying into non-scheduled operating bases by ad-hoc cargo operators.
- Operating into and from developing countries in Asia, Africa and South America, where airport facilities and processes may be non-compliant at times.
- Operating either western built old aircraft or those manufactured by the former Soviet Union, the reliability of which is poor and maintenance spares are not readily available.

Some of these factors have a flight operations bias, whereas others are particularly relevant to maintain continuing airworthiness of the aircraft. Factors such as night flying, cold weather, unfamiliar aircraft types, and unreliability in the quality of maintenance received in certain geographical regions have elements of human factors that affect the achieved level of safety from CAW process. Therefore these issues would have to be taken into account in assessing risk in CAW attributed to human error. Relevant parameters will be introduced to the risk model that would take into account these issues, and naturally data collected for the risk model will help to identify the condition under which aircraft are operated and as part of the process of mitigating the risk.

Chapter Four

Literature research - Theoretical risk assessment methods

4.1 Introduction

Continuing the literature survey, this chapter will now examine alternative approaches to risk assessment, progressing from those based on qualitative methods and subjective judgment to more objective, quantitative techniques. The aim of this chapter is to narrow down those quantitative risk assessment methods to select one that might be promising and have the potential to be developed as a risk assessment model that could meet the research objectives.

4.2 Maintenance Error Prediction Model (MEPM)

In the back drop of quite confusing mixture of risk assessment practices adopted by civil aviation, it is apt to mention some research and development work done by Howard Leach on a Maintenance Error Prediction Model[15]. His research followed in the aftermath of the serious flight incident to British Airways Boeing 777 G-YMME on 10 June 2004, 1907H, at Heathrow airport[4] described in Appendix 2.

The Leach study had been undertaken to determine how such system failures arising could be averted in future, given that the limitations of current human error management systems had failed in preventing system failure in this instance.

He observed that human emotions such as fear and apathy, as well as commercial sensitivity of operators that prevail in the culture aviation industry, and poor communication and lack of feedback undermined confidence in the existing systems. MEDA too was considered ineffective because the analysis was retrospective and failed to act on the specific maintenance task; MEDA tool also mainly recommended complexity changes within a system that relied too much on unreliable top management patronage[15]. In this background, the proposed MEPM attempts to eliminate recognized inadequacies of the present error management system.

The application of the model that comes into operation in real-time on reporting an actual or potential human error situation, works as a three-stage process, operated by an informed Expert System (ES):

a. Timely analysis of a reported occurrence or suspect maintenance task using the analytical tool, coined Maintenance Error Prediction Model (MEPM), to determine the level of risk from potential maintenance error.
b. Determining a solution to overcome or alleviate the risk, this being the defence mechanism.
c. Communicating the solution effectively to all interested parties.

An evaluation will be triggered by one of three alternative mechanisms, i.e. following an investigation of an occurrence, an engineer disclosure of a potential errant task or near miss, or routine MEDA evaluation highlighting an area of concern.

The core of the proposed system is the MEPM; it has a three-phase algorithm, against which the ES would evaluate a report of an actual error or a situation where there is a possibility of an error occurring. Each phase returns a simple numerical score from an intrinsic rating system, namely Likelihood of Occurrence of a Maintenance Error, Severity of Consequences, and Possibility of Detection of the Error.

The product of the 3-individual scores multiplied together is the overall Risk Factor attributed to the potential maintenance error, and that criterion will determine the defensive mechanism to be adopted and the urgency of action. Defensive Mechanisms are chosen analytically with another algorithm operated by ES, into which a range of defensive mechanism has been built-in.

This prediction model follows the general concept of algorithms routines used in 2 other prediction tools widely used in aviation industry: FEMA and MSG-3. Neither routine satisfactorily addresses maintenance error issues. Therefore it is envisaged that the proposed MEPM would operate alongside FEMA and MSG-3, or even as a subset of MSG-3 as this is the principal guide to maintenance requirements on civil aircraft.

The model has been validated using a sample of reported incidents. However in his conclusion Leach recommends that the model should be validated against a wider range of air transport and operating environments. He further recommends that research be undertaken to address the methods of quantification of risk as well as a number of other issues on human interface and industry culture, Regulations, Composition and Role of ES, and Company Hierarchy and Lines of Responsibilities.

The proposal has much merit in averting potential accidents by timely interaction with reported human error situations. It predicts the risk to flight safety if the situation

persists on which the urgency of action could be determined. Its limitation is that it relies on an individual or an event to discover the error initially and then to trigger the system. The model is ideal for application in near workface environment, somewhere between the tactical risk assessment level at the sharp end of operations and strategic risk assessment level at higher management.

4.3 Error Criticality Index (ECI)

Another attempt to predict risk associated with human error in maintenance has been embedded in a model researched by Simmons (2002)[16]. His proposal was to use an entity called Error Criticality Index for engineering or process tasks to determine the urgency of action if an error had occurred and left in the aircraft or its supporting documentation during the performance of the task. In fact ECI could be visualized as one of the parameters in a MSG-3 type maintenance decision matrix, with ECI bringing in another active dimension to the matrix. Note that the originator's research thesis had considered it only as a stand-alone tool with no reference to MSG-3decision matrix.

Derivation of the ECI is through a numerical process. In this, an engineering task is decomposed into small elements, and each element is then assessed against a number of criteria, on the assumption that a human error had occurred whilst performing that element. The criteria are: the effect of the error if left uncorrected at aircraft release to service, the severity of that effect, if the aircraft could physically return to service with error present, if the error would be detected by a forcing function such as a pre-take off cockpit check, where in the maintenance sequence the error occurs, and if adverse outcome has already been anticipated in the design. Assessment for each element is consolidated into the overall task through an accumulation process, and at the end of the analytical process an ECI is output.

ECI was envisaged as a value, expressed on a two-dimensional linear plot of probability of error (X-axis) and ECI (Y-axis) ranging from zero to 1.0. The number represents the importance of the plausible consequence of an event or condition. Decisions on the significance of the error can then be taken on the basis of ECI value and a threshold that might be established.

Providing some worked examples, Simmons has demonstrated the way the process works. However the proposal is fraught with some practical difficulties. Simmons recognizes that one of the limitations of the process is the dearth of data on probability of humans making mistakes in specific engineering tasks at elemental

level. For the demonstrations he uses some information output from US nuclear industry and he believes that more such data is available to the researchers. In the absence of quantitative data, he would resort to expert judgment or if not intuition.

The process is highly analytical and it is doubtful if this is at all practically applicable to a maintenance scenario, where for example a Base maintenance such as a C Check would involve thousands of engineering tasks. The problem is multiplied if an MRO handles several types of aircraft. In his research paper Leach commented on the impracticality of advance analysis of each engineering task purely on account of the vast number. It is therefore not a suitable tool for use within the maintenance organization if it involves analysis of tasks.

However, it may be a technically feasible task for the Integrated Logistic Support (ILS) Department of an equipment manufacturer or a Design Authority. As part of their normal remit ILS is responsible for the drawing up of the maintenance requirements, procedures and maintenance manuals. As such they have the responsibility to examine each engineering task critically. The calculation of ECI and how the value affects airworthiness decision would have to be taken at the development phase of the aircraft and results offered to the operators as part of Post Development Services. Obviously, the extensive analysis of engineering tasks to determine ECI would be highly labour intensive, and therefore there would be significant cost attached to a Design Authority data set that would be output.

Provided that the analytical process has been delegated to the Design Authority, the application of the model seems to be appropriate at the workface for assessment of risk due to error at tactical level. If such a system could be produced for engineering tasks, then logically it follows that a similar system could be devised for associated administrative tasks in the CAW process. Again, the limitation might be the availability of reliable data about human behaviour, and how to set up standards and threshold values. It needs further research to validate its practicability and cost.

4.4 Regulatory Oversight Weighting Index (ROWI)

ROWI model has been designed as an administrative tool to determine how best the oversight workload of the regional offices of UK CAA (the Regulator) could be best distributed amongst its inspectors in the most equitable and cost-effective manner. The model was designed by David Marsh, Deputy Manager of the UKCAA Southern Regional Office in 2006 as a private research project.

Although, his work has not been published, sufficient information was obtained during this research study in order to assess the concept. ROWI was a well-structured and documented assessment method, a positive step in the right direction. The concept of expert opinion and individual preference has been retained within the methodology.

Nevertheless, recognizing its merit, the idea of assessing an organization for its size of operation and its capability, together with some of the parameters used, has been adopted in the design of part of the CAW risk model. Thus, in the CAW risk model that will be described later, the subsystem "Size of Operation and Capability" has its roots in David Marsh's ROWI model, though conceptually the two models are entirely different.

ROWI model is in fact an EXCEL type spreadsheet composed of identified approved organizations (AOC Holders, Part M and Part 145 etc) in rows, and an array of parameters that define the size and capability of their operations in columns. The types of parameters recorded are:

For AOC Holders:

- **Capability:** Size of the operation, numbers of A1 and A2/3 aircraft operated, number of QA staff, tech planning staff, approved maintenance programs, approval of ETOPS, RVSM, AWOPS, MNPS *(Aircraft categories. A1 > 5700kg AUW or above, i.e. large aircraft. A2 = or < 5700kg. A3 aircraft are helicopters, A4 = aircraft other than A1, A2 or A3)*

- **Safety Issues:** Number of types of helicopters or fixed wing aircraft, number of aircraft in each fleet, number of MOR submitted, number of Level 1 Findings and Level 2 Findings issued over the previous year, average age of aircraft, number of operation resource variations issued over the previous year, average hours flown per month.

For Part 145 and Part M Organizations:

- **Capability:** Number of A1, Line maintenance types, A1 Base maintenance types, A2/A3 Line types and A2/A3 Base types on approval, number of B ratings on approval, number C ratings on approval, number specialized service (e.g. NDT, component maintenance etc) certifying staff employed to support

approval, number of C of A recommendations made previous year, number of AOC supported, number of QA staff.

- **Safety Issues**: Number of Form 1 (EASA – Release to service Certificate) issued over previous year, number of aircraft maintained, number of Part 145 related MOR submitted during the previous year, number of Level 1 Findings, number of Level 2 Findings issued during previous year, average age of aircraft being maintained, number of maintenance resource variations issued over previous year.

Past performance. The model takes account of the past performance as it is a good indicator of the trend of the company and its safety culture. A good return gives confidence.

Current state. Whilst considering past performance, the model takes on board any real time changes that could affect the airworthiness of the fleet or the fidelity on the organization. The latest flight or ground incidence and its root causes, error observations, their magnitudes and implications, presence of structural defects that might affect the whole fleet. These are good examples of sense of risk, despite past good performance

State of the Organization. Other organizational issues considered are: Has the AO's exposition changed, change of method of operation, equipment, CEO or even labour relationships, role of aircraft, technology etc. All these could significantly impact on the current performance regardless of the past.

Capability / Safety Issues. The spreadsheet calculates safety performance indicators for each approved organization, i.e. a Capability figure, a Safety Issues figure, and a Capability / Safety Issues ratio (e.g. 1:4.68). This represents a risk level that enables the manager to take appropriate decision on the urgency and priority for exercising oversight audits and the number of surveyors to be allocated to the task. Higher the denominator of the ratio 1: N, then the greater the importance of assigning oversight visits.

Calculation. ROWI model's internal calculation method is not visible and this research study did not have access to information on the concept used. However, its general approach, i.e. the format of spreadsheet, attributes against which an organization's performance is measured, and how data is assimilated, seems to be consistent with Multi Criteria Decision Analysis (MCDA) technique that has been described in Section

4.7. Expert judgment is exercised when the analyst interacts with the spreadsheet, but this interactive process is not available to this study. It does not matter as long as the same scale of measurement is used for each condition, and that judgment is exercised by equally experienced surveyors.

Workload Spread. Following analysis, the workload is spread out per surveyor on the basis of the summation of capability figure and safety figure of AO that is allocated to him. Naturally, some trade- off may be done between surveyors to make sure that they all get equal shares, and that the amount of travelling distance and time spent in travelling is roughly balanced out between the surveyors. The distance to the AO from the Regional Office, and the time for travel is also taken into account to determine an equitable workload between the surveyors.

Strength. The main strength of the model is that the spreadsheet takes out the largely invisible subjective judgment based on the managers or individual surveyors experience and personal knowledge of the organization. It is known that in the traditional subjective assessment techniques, the individual surveyors' personal knowledge of the system plays a major role in their assessment technique. But this knowledge is not transparent to others. However, in ROWI, such personal knowledge and information is recorded on the spreadsheet, thereby removing the variability of subjective judgment based on memory.

Thus ROWI is a management tool for the cost-effective allocation of local surveyor resources to oversight tasks. It uses the analyzed risk level of organizations represented as a Capability / Safety Issues ratio. The methodology is compatible with the requirement to implement RBO concept, even though the formula used for assessing the risk is non conventional.

4.5 Other analytical methods

Progressing from subjective judgment methods to more objective and quantitative methods, it is necessary to mention some generally known risk assessment techniques used in industry by design authorities though not seen much in practice in AOC Holder, Part M and Part 145 environment. They are certainly available in theory, often presented and discussed at conventions; they are little used by aircraft operators even though they are often used by Design Authorities.

4.5.1 FMEA/FMECA

In reliability, maintainability and testability analysis a well known technique called Failure Modes and Effects Analysis (FMEA) is used to determine the consequences of

the failure of a system, equipment, component or a process resulting from different modes of failure at lower level components. In aviation entire or parts of systems are either multiplicated or multiplexed. Therefore not all component failures lead to a system failure. However there may be certain components that could not be multiplexed for whatever reason and may remain in a critical path. FMEA facilitates the identification of such components.

Failure Mode Effects and Criticality Analysis (FMECA) which is an extension of FMEA is particularly intended to determine the criticality of such components or weak links so that they could be designed out or strengthened during the design process. FMEA/ FMECA technique usually starts as a qualitative analysis process, and once critical failure modes begin to emerge their level of resolution is increased through quantitative analysis. Where reliability data is available they could be used together with statistical methods to arrive at true probability of failures and severity of consequences converted to monetary terms, loss of business or prestige, if not to casualties. As a risk assessment tool FMEA/FMECA techniques are incorporated into the design of system diagnostic tools. This is in fact a good example of risk assessment in tactical situations; risk is already assessed within the software used in the diagnostic equipment before providing information on the details of the system error or defect.

Netjasov et al (2008)[70] discusses several other techniques utilized by Design Authorities, as summarized below. All these techniques follow the generic FMECA principles.

4.5.2 Fault Tree Analysis (FTA)

This method is used to analyzing events or combinations of events that might lead to a hazard or an event which has the potential for a serious consequence. The starting points of the tree (principal nodes) are the events in consideration. The end point is the identification of the hazard that may lead to a consequence. There may be alternative logical paths through which implications of an error in an event might propagate according to rules of combinations, “and” and “or”, through sequential stages of the business process under investigation. The probability of hazard occurring is the sum of probabilities of independent paths.

4.5.3 Common Cause Analysis (CCA)

In CCA, a sequence of events that gives rise to an accident is identified. Major equipment or a complex process is divided into zones and components (or individual

process activities) and treated independently to determine what common influencing factors or causes lead to its failure.

4.5.4 Event Tree Analysis (ETA)

Unlike FTA, where the event is analyzed to detect the hazard, here the sequences of events arising from a hazard are traced to determine the critical path that leads to the eventual consequence.

4.5.5 Bow Tie Analysis (BTA)

Bow-Tie analysis is a combination of Fault tree Analysis and Event Tree Analysis. One half of the "bow" represents FTA; several potential faults might converge into one significant hazard at the middle of the bow. This hazard then becomes the origin of several potential failure paths that diverge out from the hazard. One of the paths may be more important than the others, either because it brings out final failure during an operation, say, in a fewer number of (process) steps, or more rapidly or under lower stress conditions. This then becomes the critical path to final failure.

4.5.6 Hazard and Operability Studies (HAZOPS)

This is commercial software that is used for analyzing equipment, plant or a process to identify potential hazards and operability problems caused by deviations from its original design intent. The deviations arise from equipment malfunctions or operator human errors, or any other condition under which the design was based, for example extreme hot or extremely cold conditions from what the design was based. It follows FMEA principles, converts subjective judgment to simple linear numeric values, and come up with risk factors.

Except the Common Cause Analysis, all other analytical techniques can be quantified, provided data is available. Where data is not available assessment may be based on expert opinion (qualitative judgment) which then is quantified using an arbitrary scale and look up tables.

Numerous other specialized risk assessment models are available or have been published in research papers, most of which use one or more of these techniques in combination.

Generally all these analytical techniques are used for the prediction of significant failures, such as a catastrophic failure of a system such as a chemical plant, refinery, nuclear power station, transportation system, or an aircraft. Naturally, the analytical process for the whole system is very protracted, costly, and one needs to know a lot of input data on the behaviour of the system, and their failure modes and experimental test results. This type of exercise would be very costly, and is not catered for in this study. However, the availability of techniques has been mentioned as a research point to demonstrate different approaches to risk assessment.

4.6 Methods that quantify expert opinion or belief

The remainder of this chapter will now focus on alternative modelling techniques that might be capable of redressing weaknesses of conventional risk assessment methods and returning a realistic, quantitative output of risk.

Methodologies for risk assessment involving a human element fall into the general domain of operational analysis, and more explicitly to decision analysis. A risk model is a tool to help making decisions, and relevant modelling concepts exist in the domain of decision theory. Decision theory is a study of discrete mathematics that models human decision making and how real or ideal decision maker makes or if not should make decisions. A risk model that is likely to be accepted by stakeholders of civil aviation should be conceptually simple, practical and its methodology transparent.

There are three standard modelling techniques that can convert subjective judgment to a quantitative output, as required in this case of risk assessment in continuing airworthiness[60]. The techniques are:

- Multivariate Criteria Decision Analysis (MCDA).
- Bayesian Belief Networks (BBN).
- Fuzzy Logic (FL).

Literature survey on safety assessment in civil aviation and other industries, notably nuclear and rail also confirm that there are three strong veins running through most of the research papers; they too converge on these three modelling techniques.

4.7 Multivariate Criteria Decision Analysis (MCDA)

MCDA approach seeks to take explicit account of numerous conflicting criteria that affect a situation in aiding decision making. The principle aims of the technique are to

help decision maker explore the problem situation, learn about their own and others values and judgments and identify a preferred course of action.

MCDA technique has a number of key elements. First the problem should be identified. More often than not it is a decision problem, e.g. to select one course of action out of several possible options. Then the decision maker should be identified, together with the alternatives from which one has to be selected. The attributes of each option should be identified together with the objectives as well as threshold values of the requirement that each option must meet in order to pass. If there are no such thresholds, there must be rules for evaluating the performance against attributes (or criteria) so that it is possible to discriminate between possible options, e.g. select the method that is the simplest to operate and demands the least labour.

The process of applying the technique involves the setting up of a spreadsheet or a matrix (Table) of alternatives in columns, and attributes in rows, see Table 4.1. Attributes that are essential to the solution are placed at the top half of the matrix irrespective of the rank, and other desirable criteria in the bottom half in order of importance. In addition to ranking the desirable attributes, they may be weighted according to their importance to the purpose for which a selection is made.

Using the matrix and available information, each alternative's performance is then assessed against each attribute. The performance may be numerically scored according to a pre determined scale and weighted. If there are more than one decision maker, then it is normal to seek consensus because the evaluation of performance could well have a degree of subjective judgment. Similarly there should be consensus amongst the decision makers about the rules for weighting.

By combining the attribute weights with the scores for each alternative, it is possible to produce an overall weighted sum or an average for each alternative. Obviously any alternative that does not meet essential objectives or thresholds are eliminated. A decision may be made by selecting one option from the remainder, which offers the best alternative according to the weighted scores.

This technique could be used to assess the relative risk level of a number of approved organizations and to rank them, this being the desired solution to the decision problem. The alternatives are the approved organizations, and the attributes are the criteria on which risk level is evaluated. In the ROWI model described in Section 4.4 the attributes are the features that define the size of the operation, capability and safety issues.

Alternatives / Attributes	Weighting	AO 1 Info	Weighted Score	AO 2 Info	Weighted Score	AO 3 Info	Weighted Score	AO4 Info	Weighted Score
Size of operation									
Type of aircraft									
No in fleet									
Role									
No of B1LAE									
No of B2 LAE									
Sectors flown/ yr									
Sectors/ac/day									
Etc ……									
No L1 findings									
No L2 Findings									
ETOPS									
RVSM									
Ac average age									
LAE/ac ratio									
LAE/Managers									
Num MOR									
MOR cleared									
Num MEMS recorded									
MEMS recorded/MEMS not cleared									
Etc…									
Score									

Table 4.1 – Specimen MCDA matrix

In this exercise, if the criteria are well defined and a value can be attributed to it, the scoring process becomes easy. But if some or all of the criteria are unclear and attributes could have more than one possibility, or more than one person express opinions on what is the correct value to use, then this type of problem solving

becomes harder. Invariably, to handle such situations, MCDA technique has evolved into more complex versions incorporating various refinements.

For example, where opinions of more than one expert have to be considered, Delphi Technique[71], developed by the Rand Corporation in the 1950s, is used to eliciting information from a group of people and refining the opinions iteratively until a consensus is reached. Anonymity between participants must be maintained to eliminate bias. If the group is large, statistical measures may be used to assimilate and analyze the responses to iterations. Unfortunately this need for opinions from a larger group of people makes MCDA somewhat difficult to implement in an industrial set up where labour is a premium asset.

	A	B	F	G	H	I
1	147 BT	Surveyor				
2		2nd Surveyor				
3		Date				
4		Approval nr.				
5		Company				
6	Compliance with Part 147 req.	147.A.100 Facility requirements				
7		147.A.105 Personnel requirements				
8		147.A.110 Records of instructors examiners and assessors				
9		147.A.115 Instructional Equipment				
10		147.A.120 Maintenance training material				
11		147.A.125 Records				
12		147.A.135 Examinations				
13		147.A.145 Privileges				
14		147.A.200 The approved basic training course				
15		147.A.205 Basic knowledge examinations				
16		147.A.210 Basic practical assessment				
17		**Compliance with Part 147 req.**	0	0	0	0
18	Quality System	147.A.130 Training procedures and quality system				
19		147.A.140 MTOE				
20		Prestaties klachten en incidenten				
21		Niveau / afstemming K-systeem				
22		**Quality System**	0	0	0	0
23	**Quality Risks**		0	0	0	0
24	Organisation culture & society	Attitude to faults, incidents and risks				
25		Political, social interest				
26		Communication and relations				
27		Recruitment policy and personnel exp.				
28		Upholding rules	PM	PM	PM	PM
29		**Organisation culture & society**	0	0	0	0
30	Organisational features	Complex organisational structure				
31		Location Control				
32		Farming out tasks				
33		Hiring personnel				
34		Stability of organisation				
35		**Organisational features**	0	0	0	0
36	Compliance with Part 145 req	Production volume				
37		Product complexity				
38		Product variation				
39		Innovation, changes				
40		**Compliance with Part 145 req**	0	0	0	0
41	**Organisational risks**		0	0	0	0
42	**Risk level**		0	0	0	0
43						
44	**Number of inspection before RA**					
45	Inspection coeficient		0,25	0,25	0,25	0,25
46	**Number of inspection after RA**		0	0	0	0

Table 4.2 – Portion of specimen AHP matrix used to assess Part 147 TO (Source: CAA-NL)

A further version incorporating Shang Enquiry[72] enables an individual expert to express his opinion but relaxes the way he could answer, say with a discrete or variable range with a min and a maximum value.

Analytical Hierarchical Process (AHP) or Saaty Technique[73], as it is alternatively known, allows canvassing opinions from several assessors, weighting of criteria, and pair-wise comparison of criteria as a means of eliciting information on the way assessors pace importance on the criteria that defines the organization's behaviour. A particularly good example of MCDA/ AHP technique application can be found in the risk assessment method used by NL-CAA. AHP is much more complex process. Table 4.2 demonstrates part of a specimen matrix used to assess risk of a number of Part 147 Training Organizations.

MCDA, together with its different advanced versions, is the most popular method because people can easily relate to the technique without the necessity for a deep theoretical understanding of the subject; it is practical and allows subjective judgment to be exercised. However the drawback is there is a degree of subjectivity when assessing performance against those criteria that cannot be defined with numeric precision and in determining the weighting to be applied to certain criteria.

4.8 Fuzzy Logic (FL)

Decision making in real life has a degree of vagueness because not all input information that contribute to the decision making are precise. Even though some information appears to be precise, they too are subject to continual change. This dynamic nature of states of affairs in the real world, together with the inability to know all the conditions that influence the decision, brings about an uncertainty to the decision making process. Therefore it is very common for the decision maker to express his decision with an expression of vagueness. Thus on a decision on risk, he might say that "given certain conditions, releasing an aircraft to service is unlikely to be at risk".

Mukaidono (2001)[74] provides a simple introduction to Fuzzy Logic without formulae. Examples of Fuzzy Logic are the people's behaviour to normally immeasurable physical conditions, such as coldness, because it depends on the feeling of the one who expresses it. One person's coldness may be another person's hotness. Similarly, a person's sense of bad risk is another person's good risk and opportunity to make a profit. Judgments expressed in terms of, "unlikely", "fairly possible", "highly plausible" are ambivalent and indicate mental conflict of uncertainty. In fact, the logic

of Fuzzy behaviour can be organized as Fuzzy Logic and represented as a mathematical way of handling imprecise concepts involved in subjective judgment and abstract expressions of this nature[75].

It can be seen that Fuzzy Logic deals with possibility rather than probability, and uses approximate reasoning rather than precise, leading to the use of imprecise concepts and linguistic expression like, “slightly”, “quite” and “very”. Coincidentally, the qualitative definitions concept used in the risk matrix (see Chapter 3) as recommended in ICAO SMS, has many expressions that are in common with those convertible to numeric values with fuzzy logic.

In the workings of FL model, for example in a risk model, the imprecise information expressed as expert opinion of risk may be converted to mathematical expressions and operators (e.g. Boolean logic)[76]. The conversion is done through a graphical representation of the fuzziness (vagueness or imprecision) between the two extremes values as a sloping line, whose gradually varying points are read across to a scale between 0 and 1, see Figure 4.1. The varying points represent different degrees of vagueness according to the person who is making the judgment. Thus in a risk assessment situation, the subjective judgment could vary from one extreme to having “No Risk” to the other extreme “Definite Risk”, and in the intermediate range low risk, medium risk or high risk. The boundaries between low risk and medium risk, or between medium and high risk are not clearly defined, as they depend on the viewpoint of the decision maker.

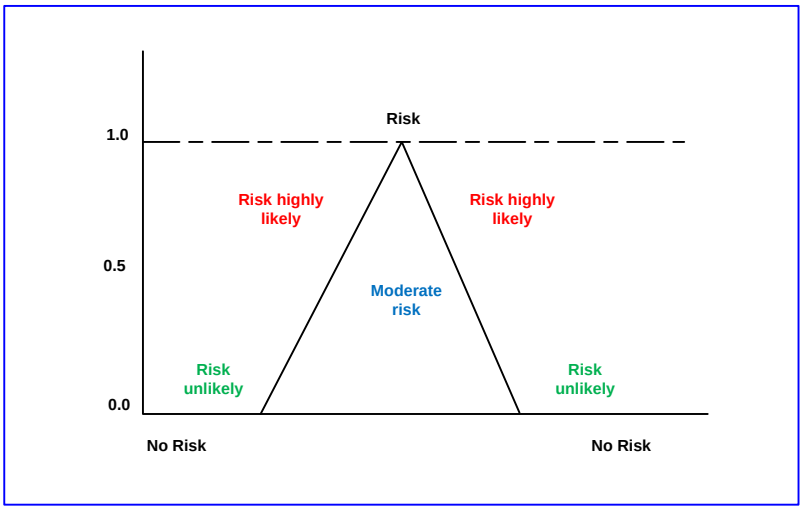


Figure 4.1 – Representation of vagueness with Fuzzy Numbers

In a process involving a series of engineering task, for instance, the process would have to be analyzed task by task to determine each task’s risk contribution, using a

standard risk assessment matrix. If FL is used in that situation, the parameters probability of a hazard and severity of consequences that are usually defined subjectively in vague terms would have to be converted to Fuzzy numbers. If MCDA or AHP technique is used for assessment, then evaluating performance of the alternatives against attributes would need Fuzzy numbers if these attributes are defined subjectively and with imprecision.

Thus FL requires an entire new range of words and expressions used to define measurement of performance against attributes, or to define conditions and objectives, all written in Fuzzy Language and their conversion to Fuzzy Numbers. The language has expressions in the Boolean of Logic, e.g. IF X AND Y THEN Z. The full rationale for the derivation of Fuzzy Language and the mathematical analysis of the conversion to Fuzzy Numbers is outside the remit of this study but they could be studied in standard text books on FL[75].

McCarthy et al (1999)[77]reports on an internationally known research program Flight Operations Risk Analysis System (FORAS) in which both AHP and FL concepts have been utilized. The objective of FORAS was *"to generate a risk model which produces a relative, quantitative measurement of a specific risk exposure in flight operati*ons". "*The model represents risk factors and their inter-relationships, and to risk. The generic model may be applicable to all situations of flight operations that lead to accident, e.g. mid–air collision, CFIT and runway incursion etc. The method is a structured approach to eliciting and representing domain experts' knowledge, and then converting it to produce numeric risk outputs, where FL concept comes into play. FORAS is a decision support tool to measure and reduce risk exposure".*

In the field of maintenance Hamad (2010)[78] has reported on an Aviation Maintenance Monitoring Process (AMMP) which models risk associated with helicopter maintenance activities in the field. FL concept has been utilized in the mathematical analysis of the model that returns a numeric value of risk, converting subjective judgment of domain experts.

4.9 Bayesian Belief Networks (BBN)

Where there is a degree of uncertainty, belief networks enable reasoning to arrive at a decision and to solve a real-life problem. When a belief network utilizes Bayesian statistics on mathematical probabilities of events happening or not happening in a given population, it is called a Bayesian Belief Network (BBN).

BBN is a utility, a statistical tool, which estimates the state of nature of an event when the true state of nature is hard to know in the face of uncertainty. The tool helps a manager with decision making, the way it should be done, even though the BBN itself will not take the decision for him. It is the responsibility of the manager to take the appropriate decision, first having weighed up the indicator from BBN against all other factors, such as financial information, if they are not incorporated into the BBN because he wishes to keep them information separately.

The basic concept behind BBN is rooted in Bayesian Statistics, originating from Bayes' Theorem of conditional probability, which was attributed to Reverend Thomas Bayes (1702-1761AD). The theorem explains the probability of an event taking place when quite separate contributory factors to the event that occur independently turn out to have a dependency because they are related through the event. In this circumstance the two factors have a D-Separation, or Dependent Separation, as their relationship is defined. D-Separation is explained at Section 4.9.1. BBN works on this principle.

In modern times, the revival and development of Bayes' Theorem as a practical tool for applications in complex systems has been led by Judea Pearl in the 1970s in his research work into artificial intelligence[79] A helpful introduction to the topic has been made by Jensen (1996)[80].

BBN appeals to the realists, because its key feature is that it models cause and effect, and it represents a part of the world that exists around us. Since real life events occur as part of a chain of events, the downstream events are conditional upon what has happened at the preceding upstream point or some other points before that, or combinations of them. Therefore there is a conditional probability of the event happening, depending on prior probabilities of other events happening elsewhere in its causal chain.

In BBN events leading to decisions are initially presented as an Influence Diagrams (ID) as they are commonly called, which are in fact a form of causal chains. These causal chains are similar to Event Trees or Fault Trees introduced in Section 4.5. An ID resembles a neural network, where nodes incorporate the states of an outcome that was dependent on upstream causes. A very basic network is at Figure 4.2. Each node represents all the states that can exist of the event and their probabilities of occurrence.

Nodes are connected by links in a rational manner, according to their relationship in the process or system that they represent forming causal chains of events. The links

are called “arcs”, and indicate the dependency between variables, with the arrows indicating the direction; the upstream node is the “parent” and the downstream, the “child” . Thus, a causal chain has a direction; nodes have a sequence, and a relevance or relationship according to their functionality. Such a network is called a Directed Acyclic Graph (DAG); directed meaning the flow has a specific direction. Being “Acyclic” a DAG has no feedback loops, although they allow shunt lines, according to the rules of the BBN concept[80].

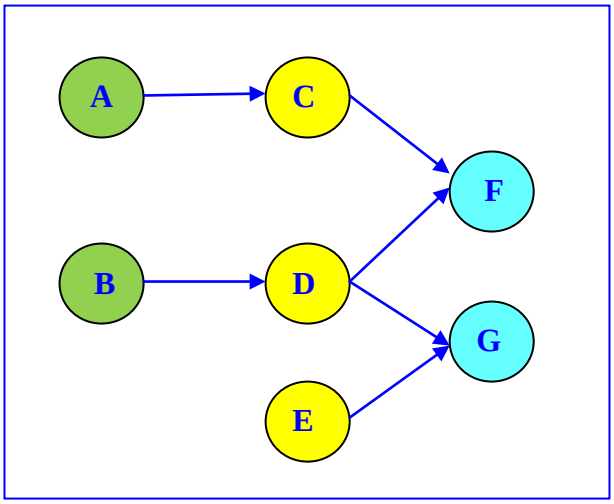


Figure 4.2 – A basic Bayesian network

The nodes are called the variables in the process system. Embedded within the nodes are descriptive and statistical information on the event and its states of nature.

There are two types of nodes: random or chance, and deterministic. For a random variable, the probability distribution of output is known for a fixed set of inputs. A deterministic variable (DV) is one which has the same output value for a fixed set of input. DVs are less common than RV.

Most BBNs that provide information to managers may contain only chance or deterministic nodes. Some networks may contain a utility node , or utility node as well as a decision node; these are called influence diagrams (ID).

With the mathematical manipulation of information contained in these networks, it may be possible to infer other “what-if” information on the behaviour of the overall process, or to interrogate what would happen at other nodes that represent upstream or downstream events.

4.9.1 D-Separation

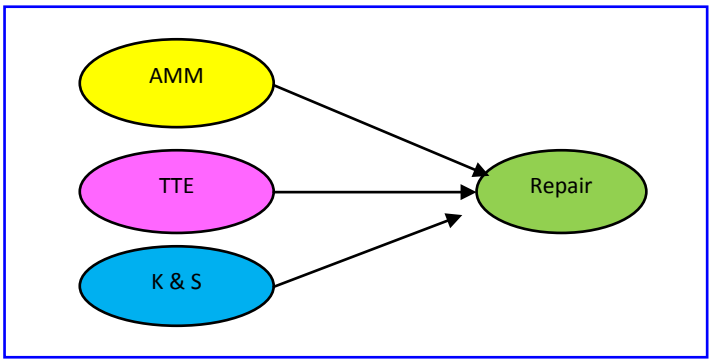


Figure 4.3 – D-Separation of contributory factors to repair

If two or more naturally independent nodes are connected to an apex (child) node, then the parent nodes are considered D-separated if they have a dependence on one another on account of the fact that they have a relationship through the child.

For example, consider the situation depicted by Figure 4.3 where a repair has been undertaken and that the state of the outcome of the repair has been influenced by the state of information presented in the Aircraft Maintenance Manual (AMM), the serviceability state of Tools and Test Equipment (TTE) and the state of Knowledge and Skills (K&S) of the engineer. This relationship is represented by the network, where the child node represents the state of repair, and the parent nodes represent:

- State of Aircraft Maintenance Schedule
- State of Tools and Test Equipment, and
- State of Knowledge and Skills of the engineer.

Each of the 3 parents can have the states, “satisfactory” or “unsatisfactory” independent from any of the other two parent states. Each parent contributes to the State of Repair, and the only reason they are inter-related is through their involvement in the repair process.

Now, assume that initially only two of the three parents are contributing to the repair, and the repair was “unsatisfactory”; if it was known that AMM’s state was “satisfactory”, then that information alone gives us information on the state of Parent 2 (TTE), that being “most likely, unsatisfactory” in order to give an “unsatisfactory” state to the Repair. Thus, though the two parents were independent and separated in their own existence, in this situation they have become dependent; therefore D-Separation rule applies here.

If the third parent "Knowledge and Skill of the engineer" is now linked to the child, then knowledge on one parent leaves 2-possibilities of states on each of the other two parents. And a further knowledge of one of them would enable the 3rd parent's state to be determined.

This dependence separation of parent nodes is an important concept when determining causal chains.

4.9.2 Conditional probability

In BBN, computation gives a quantified statistical probability. Probability may be based on statistical data on measurements, observations of actual events taking place, or if not on estimations made by experts based on their opinion or judgment.

If the probability so obtained is the "absolute truth" about its probability of happening or not happening, is a moot point. This is because software programs written for handling data may have certain techniques incorporated into them so that "zero data" could be handled according to the way nature expected. More about this will be said later, when it comes to handling data and discussing results.

The other issue that influences "absolute truth" is this: the truth of a situation might not be ascertained until all the conditions or prior events have been audited for their effect on the situation. This is correct; but then one might question, how one could be sure if all the conditions had been taken into account?

There is in fact no way one could be absolutely sure that all conditions have been taken into account. One could take into account only those in one's informed knowledge, and knowledge is limiting. To be realistic, one should in fact admit that there are more things that one does not know about the world around, than what one knows about it. New information might come to light, later on, but it is not possible or practical to wait for the new information to arrive. Meanwhile one should make the best estimate based on information available, and readjust the result once new information is known. BBN allows this flexibility; it calculates for present known conditions and allows new data to be input at a later stage when that is known. If necessary the BBN structure may have to be modified in response, or leave an allowance in the calculation as a safety factor to allow for the unknowns.

To make probability calculations, information about the events that constitute the causal chain, which is now the ID, would have to be embodied into the ID. This

embodiment is done at the nodal points of the ID. There are two types of data embodied there. One is the natural state of the outcome of an event, and the other is the probability of that outcome.

As explained before, states of nature at the nodes and probability data may be based on observations and measurement of actual events, or judicious estimates based on knowledge about the processes. It might be possible that data for all nodal points might not necessarily be available. In that case, as much nodal points as possible should be populated, and the network should then be able to calculate the missing information. But it would work only if the correct logical outcome of events at the nodal positions were known and inserted; that is why the fidelity of this operation is expert dependent.

Once this embodiment was done, and the missing data were calculated, then the ID would have been converted to a BBN, as well as it had been primed with prior probabilities of the states of nature at nodal points. Calculations on the BBN are done either manually or digitally on a computer using appropriate software.

4.10 Advantage of BBN over other techniques

The way BBN has been applied in risk assessment attributed to human error will be described in detail in the next two chapters. Here some qualitative statements are made by way of an introduction.

BBN was originally intended for use with information on individual beliefs. But it has a unique quality that actual real life data on error observations can be used in the model. Where data is not available, individual beliefs could be substituted to start with, but as data begin to arrive, they could be used to replace beliefs. BBN encourages evidence to be recorded in future, to replace subjective assessment with evidence, and so to improve the fidelity of the assessment process.

Since BBN technique incorporates proper statistical calculation to determine probabilities, it provides a capability to move away from qualitative expression of risk and put actual numbers. This is irrespective of the fact that the probability distribution of states of nature at nodes is based on evidence or if not on expert opinion.

In fairness, it should be stated that some other techniques such as Fault Tree Analysis (FTA) are also amenable to statistical analysis, outputting quantitative values.

Unfortunately, in FTA, a complex process such as continuing airworthiness could result with a huge table of all probabilities and combinations. In contrast BBN takes only those probabilities which are causally dependent, hence enormously reducing the computing power requirements. Any one node will work only with related family, "parent-child" nodes.

Input arrays		1	1	A=4 feeds into C	B=4 feeds into D	1	C=4, D=4, i.e. 4x4 feed into F	D=4, E=4, i.e. 4x4 feed into G
Variables in each node	4	CPT 4x1 =4	CPT 4x1 =4	CPT 4x4 = 16	CPT 4x4= 16	CPT 4x1 =4	CPT 16x4 = 64	CPT 16x4 = 64
Nodes		A	B	C	D	E	F	G

Figure 4.4 – Representation of Conditional Probability Tables for nodes in Figure 4.2

One of the main advantages of BBN over other similar graphical presentations (e.g. a decision tree, an event tree or fault tree) is this simplicity. For example, if each of the variables in the above network at Figure 4.2 has four states, then 4^7 (=16,384) probabilities would have to be specified for a fully connected dependent structure, whereas only 172 would have to be specified given the conditional independence. Figure 4.4 represents the layout of the elements in a Conditional Probability Table (CPT) for each node, i.e. A = 4, B=4, C=16, D=16, E=4, F=64, G=64, giving a total 172.

Networks are also adaptable and modified to suit the occasion. For example, initially the net work may be small to cover the known processes and information, but later the network can be expanded as experience is gained. There is also no need to have all the knowledge about the process system, as BBN can calculate for nodes where data is missing.

The capability to transit from qualitative expression to quantitative is an essential research objective for a risk model. It also encourages stakeholders of civil aviation to shift from existing known risk assessment methods to something they were, hitherto, less familiar with.

In a people orientated phenomenon such as risk assessment, new methods should be introduced with caution. It is hoped that BBN techniques that provide the gradual transition from qualitative to quantitative methods can impart confidence in the stakeholder, as the technique is transparent and they can judge if the results are meaningful.

Given these considerable advantages of BBN over other techniques reviewed in this survey, BBN is the obvious choice for the way forward. Vagueness is replaced by actual events, error incidents, consequences and their impact; as such there is no need to express uncertainty with words; there is a precise statistical probability. Therefore BBN surpasses FL or MCDA in providing a more realistic representation of the state of uncertainty at any application.

4.11 BBN applications

Artificial intelligence, robotic controllers, medical diagnosis and prediction, and control of eco-systems are some domains where BBN are widely used. In aerospace and defence sector, BBN is known to be used in sensor and data fusion, weapons effective assessment, defence aids and countermeasures to name a few. Most general research papers that mentioned these applications were prescriptive; they were not informative about the way a concept could be converted to a working model.
Those few research papers that predict the possibility of Bayesian techniques in action in aviation largely focussed on the application of Bayesian statistics to engineering problem solving, which is different from the application of Bayesian Networks.

4.11.1 Un-airworthy despatch

For example, reviewing the causal factors leading to unairworthy despatch of aircraft after maintenance, Patankar et al (2003)[81] had utilized Bayesian statistics to determine the relationship between consequences, types of error and causal factors.

He has looked into some 937 incidents on aircraft from US civil aviation, reported to FAA during the period from 1996 to 2000, of which approximately 40% fell into the category of maintenance error incidents. His analysis brought out 11 different categories of consequences, 11 maintenance error types and 25 potential causal factors. Prior probabilities were calculated, and then, the bias of causal factors was determined given that a specific consequence has occurred.

In this Patankar et al was using Bayesian Techniques as a diagnostic tool for the prediction of most likely causal factors, given that a certain flight consequence has occurred. For example, the lack of awareness was 22 per cent of documentation errors, whereas documentation errors were 33 per cent of all non-airworthy dispatches. Similarly poor procedures contributed to 4.1 per cent. Patankar used straightforward Bayes' Theorem and a basic custom design computer program to

speed up calculations. There was no indication as to why more sophisticated BBN software was not used, as they were available in the market during that period.

Again Patankar's study was based on incidents reported by different airlines in isolation, and in relation to the overall incidents that occurred in the civil aircraft operators throughout the US. For this reason, they cannot be used to measure the integrity of any one airline, and hence is not practicable as a management tool though it gives an indication of the general state of health in US civil aviation regarding dispatch of aircraft considered unairworthy due to the presence of maintenance errors.

4.11.2 Particle Swarm Optimization (PSO)

Another application, this time of BBN rather than Bayesian statistics, has been cited in a paper by Sahin et al (2007)[82.] This is a highly analytical paper describing a tailor-made, specialized Bayesian Network called distributed Particle Swarm Optimization (PSO) that utilizes performance data from an airplane engine to determine the incidence of error in its performance. Thus, PSO is a diagnostic tool that can be used to predict engine faults. Part sponsored by Honeywell Inc, Minneapolis, USA, a reputed Design Authority for aircraft and engine instrumentation systems; this research may be in support of a future engine real time health monitoring. Engine fault diagnosis equipment such as those used on Digital Engine Control Unit (DECU) for application in a maintenance environment is an alternative application.

The key issue discussed in the paper is learning the structure of the network from multitudes of sensor data coming from the engine. It is a highly academic paper that dwells on programming of software, data handling and in depth structural learning from data issues. The authors claim that, within the remit of their research study, they have successfully implemented a fault diagnosis technique for airplane engines. A network with the best inference BN generated by their PSO software has been presented in the paper.

4.11.3 Aviation System Risk Model (ASRM)

A more relevant application of BBN to forecast error probability in maintenance has been developed by Luxhoj (2002)[83]. He demonstrates an Aviation System Risk Model (ASRM) based on a BBN at its root level.

The scenario set for this paper is aircraft maintenance. The network at the heart of the ASRM represents the key influencing factors for a repair process of a maintenance organization and its outcome. The BBN maps the Reason Model[1], identifying factors that are attributable to the organization, task and its environment, individuals at workface and finally to the final outcome of the process and consequence of error, if any. It is a simple model with only 14 nodes, whose architecture is based on learning specific accident case histories and the reversed engineering of causal chains.

Thus, in generic form, ASRM represents the interrelationship between errors, consequences and causal factors, which has been matched to a Bayesian Belief Network. Causal chains indicate that root causes may lie, not necessarily at the individual work face alone, but equally on errors in task definition, in organization or in combinations i.e. obeying the concept of Reason Model.

ASRM can be used to quantify the risk level existing at various nodal point of the network in response to a variable input. The risk level is the probability of the intended resulting consequence. Provided that some of the probabilities of such upstream states or events could be estimated for some of the constituent Nodes (or states) of the model, then the final outcome of the consequences could be computed. In this model risk is defined in terms of the probability that a certain failure could happen (this being the consequence) if upstream airworthiness activities or network elements were found to be faulty or erroneous.

The model has been validated using data collected from a repair/production facility for a major component of the aircraft empennage structure. He has used data from 16 case studies of the same type of components, undergone repairs in the production line of a repair organization.

Other papers by Luxhoj[84] covered the same principle and were further illustrations of relationship between various causal factors, sources and risks

The principal strength of Luxhoj's technique is that it demonstrates a possible methodology for quantifying and computing causal factors and consequences in aviation applications. Once a network was set up it can be used repetitively and with ease.

Luxhoj sets a good precedence to follow in relation to BBN as a powerful risk analysis technique. However details of the rationale for the design of the model, the design, construction, data collection and data handling aspects of the model were missing

from his research papers, making this line of enquiry an interesting research challenge.

4.12 Preferred modelling concept

This study has considered circumstances under which risk is assessed in CAW of air transport, i.e. tactical level, strategic level and at regulatory oversights. It has also examined risk assessment techniques ranging from the traditional subjective methods to various theoretical concepts.

The study found that the variability of conditions at workface, unexpected or unplanned situations, time pressure together with business objectives make the expert human operator the best medium for assessing risk at tactical level. They may be supported with pertinent information from system diagnostic tools, into which real time equipment reliability and risk models have been integrated.

Assessing risk as part of CAW management process, a model might be of help if it has already been either programmed to cover all known conditions or has flexibility to adopt to change. Moreover, reviewing the two industrial requirements, i.e. implementation of SMS and application of RBO of Regulatory compliance, it is clear that a model designed for strategic level applications would best serve both requirements.

Each of the three modelling methods from Decision Theory, i.e. MCDA, FL and BBN, could give quantitative outputs, but it is only BBN that could return a statistical probability. Other two methods return quantities that are simply yardsticks for measuring risk; they may be useful for making comparisons as relative numbers, but they do not convey the true meaning of risk as a statistical probability of a consequence.

Risk values returned by BBN are absolute values and have a practical significance, and should be more meaningful to an Accountable Manager. That, together with the greater accountability and transparency of the logic, the way risk level decisions are arrived, and above all the simplicity of technique above FL, makes BBN the preferred concept for the risk model.

Chapter Five

Methodology

5.1 General outline

Despite conceptual research studies by Luxhoj[83, 84] BBN appeared to have made little progress into aviation applications. It seems that not enough has been done to convince the safety experts of high level organizations such as ICAO that set the direction of international civil aviation safety policies on the merits of BBN as a risk assessment modelling concept. The industry's reticence to acknowledge BBN might have been partly due to the lack of research data bridging the gap between a pure concept and a practical application, and partly due to the natural doubts and objections to new ideas coming from the traditionalists.

In this backdrop, the research work described in this thesis serves as the bridging link between the concept and an industrial application. Table 5.1 highlights the principal differences between ASRM and CAW Risk Model.

ASRM	CAW Risk Model
Conceptual and academic, exploring the potential for BBN, thus subjective. Papers devoid of methodology.	Adaptation of the concept for an industrial application, thus objective. Methodology derived from first principles. Provides a fully traceable methodology, design algorithms and a progressive guide.
Scope of the model limited to one specific engineering task. Tested and validated using few human error cases on the same component.	Scope much wider scale. Model covers an extensive CAW process involving multitude of tasks, different aircraft, personnel and a range of CAW related organizations, error sources ranging from the workface to global influences. Heuristic approach. Tested, and validated using field data representing a wider population of error sources.
Fixed form architecture	Generic in order to make the model and technique suitable for universal application, yet flexible enough to adapt it to specific organizations. Modular construction to enable add-on or truncation.
Low resolution dictated by small number of nodes and causal factors. Simple model.	High resolution. Large number of nodes and causal factors. Complex model.
No information on data requirement and handling	Investigated data requirements, collecting data and data handling.
Applicability left open.	More appropriate for risk assessment at strategic level.
	Potential for adaption in other specialist areas of civil aviation: flight operations, airfield management and ATM

Table 5.1 – Comparing ASRM and CAW Risk Model

The CAW Risk Model's strengths, limitations and the research study's contribution to knowledge are described in Section 10.6 to Section 10.9.

5.2 Methodology overview

The methodology adopted can be perceived from two aspects.

- First, the high level perception that dealt with the general approach to the problem solving and how to reach the project objectives.

- The second is a closer perception with better resolution, of the detailed methodology employed in the design of the model. This is the core task. It has been further explained in a subset.

There is a much deeper third-level to the methodology but it will be discussed in Chapter Six in the design of the model, where it is more appropriate when handling detailed modelling issues.

5.3 High level perception

In the high level perception, the project objective was considered along with potential technical solutions to determine if a solution is feasible from existing knowledge, expertise, precedence and resources. If not what other new directions are available and ought to be explored.

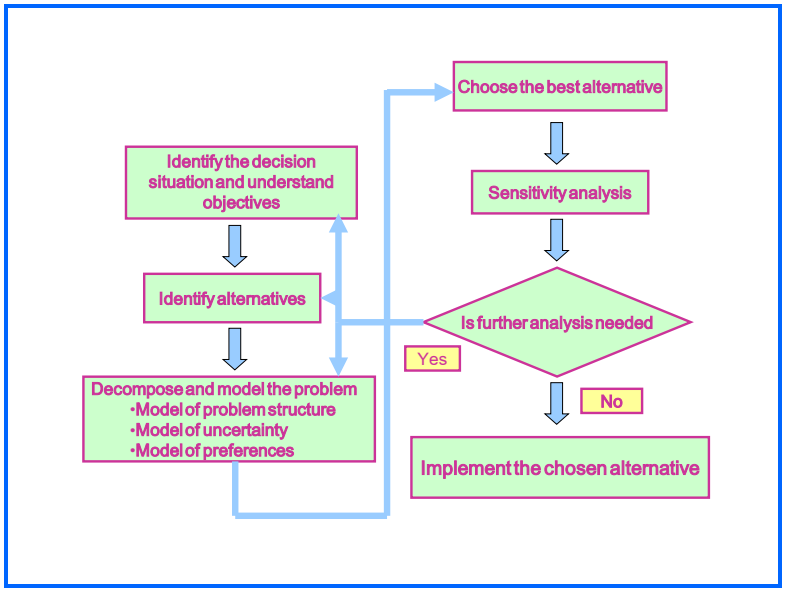


Figure 5.1 – General problem solving methodology

This preliminary research phase identified air transport industry requirements as well as potential risk assessment concepts, matching one of the concepts against one of the requirements from which an application was found. This phase was undertaken through literature research, studying the practical and political aspects of the industrial scenario whilst undergoing the industrial attachment.

This phase followed the general problem solving method outlined in Figure 5.1, as per Clemen[85], and slightly modified. The flow diagram was a good guide

Figure 5.2 represents the overview of the project by the time the study has progressed up to the point of selecting a modelling concept. Section 1.6 and Figure 1.2 outlined the activities and methodology for arriving at this point.

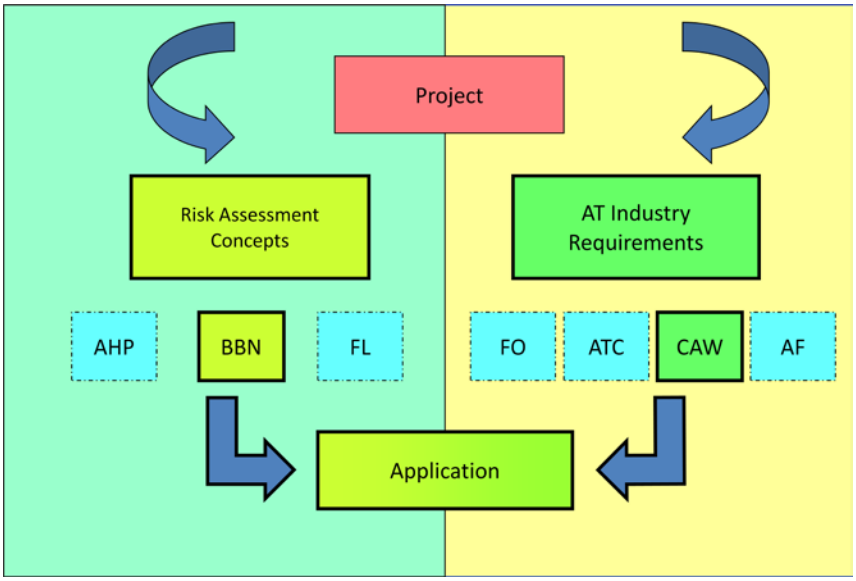


Figure 5.2 - General approach to the selection of a modelling concept
Key: AHP Analytical Hierarchical Process, BBN Bayesian Belief Networks FL Fuzzy Logic, FO Flight Operations, ATC Air Traffic Control, CAW Continuing Airworthiness, AF Air Field Management AT Air Transport

In Figure 5.2, CAW is recognized as one of four essential operations that uphold flight safety, the others being high integrity of Flight Operations (FO), Air Traffic Control (ATC) and Air Field (AF) environments. Full flight safety could be assured only if risk is either eliminated or reduced to a tolerable level in all four areas.

In this study the CAW aspect has been singled out for investigation, to determine how its contribution to the total risk could be assessed. The initial design, a generic model, was expected to demonstrate the validity of the application of the model in a CAW

environment. With this objective uppermost, the model was tailored to accept CAW process related error data without sacrificing its generic nature of the structure.

Having surveyed relevant literature, current risk assessment practices and alternative methods, the field of potential concepts has been narrowed down to three, namely: MCD/AHP, FL or BBN. Their analysis and evaluation against industry requirement has led to the selection of BBN as the concept that best fits industry's foreseen risk assessment needs, as perceived by this study.

In high level perception, as represented in Figure 5.3, it was envisaged that the concept proven model in CAW environment could be used as a guide to developing risk models in other areas. It was assumed that:

- The nature of people employed in flight operations, ATC and air field services management is no different to those handling CAW processes when it comes to making errors in industrial settings.

- The relevant specialist processes could be decomposed to events and states of nature, similar to the way they were decomposed in CAW processes. BBN theory already acknowledges this possibility for any process.

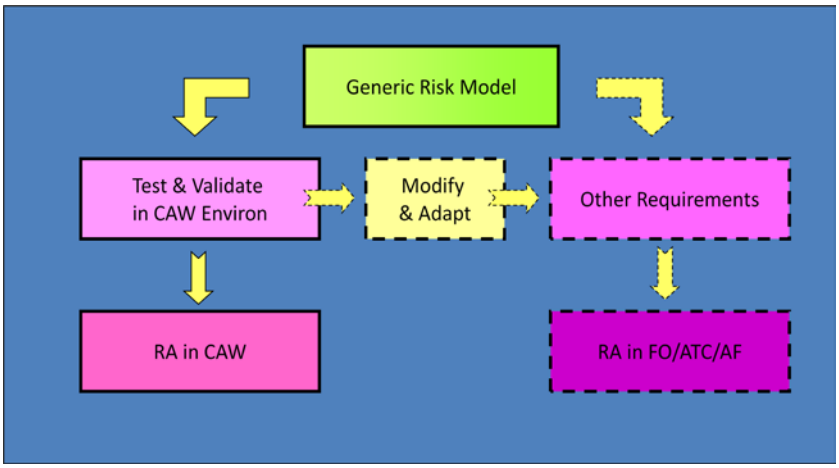


Figure 5.3 – Evolution of variations from a generic model

This extended research for the evolution of variations was not undertaken within the remit of this research program, but left as a topic for future research.

In the high level perception, once a concept was selected, detailed analytical work followed into model design phase. The end of Chapter Four defines this demarcation

line. The preceding high level perception of the methodology is given by way of orientating the reader into the overall plan.

The next major task from this point onwards was to develop the generic risk model and then to take the model forward through testing and then validating in the field. All this work was implemented though several distinct work packages, i.e. design analysis, model design, testing the model and validation, undertaken in Year 2 and Year 3 respectively (Figure 5.4).

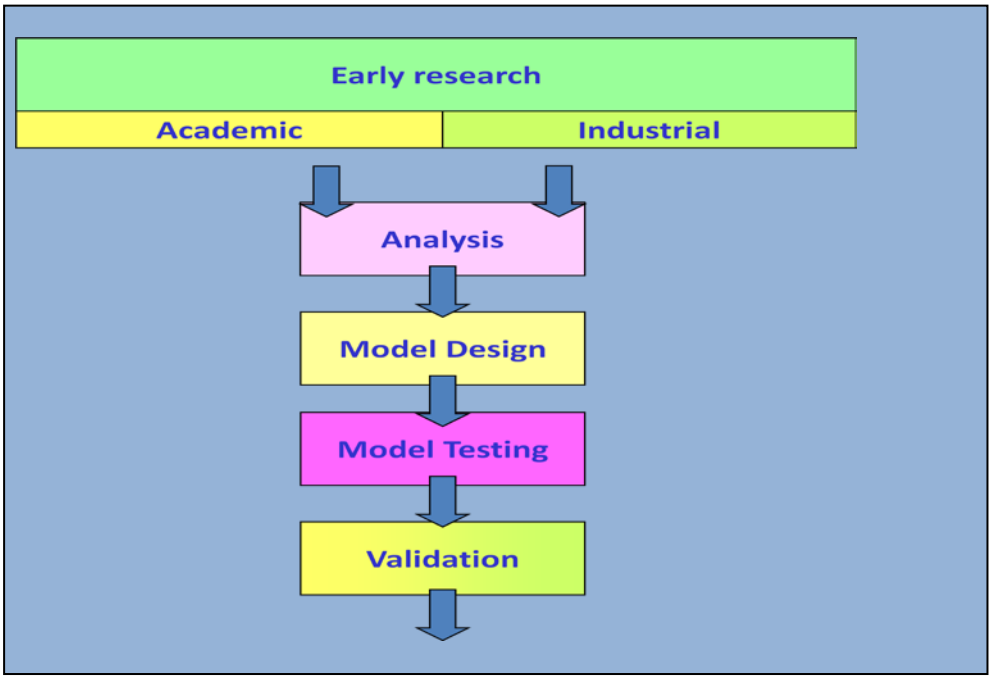


Figure 5.4 – Work packages and flow process to validation

5.4 Intermediate level perception for model design

The model design was a very complex process; an intermediate level overview of the methodology adopted is shown in Figure 5.6. It is one way to get to the objective. There may be other ways and future researchers need not necessarily follow this method every time.

The analysis phase constituted establishing the relationships between Bayesian concepts, CAW process activities and defences against malpractices of operation enforced by Regulation. The phase involved Bayesian learning, learning CAW processes and Regulation.

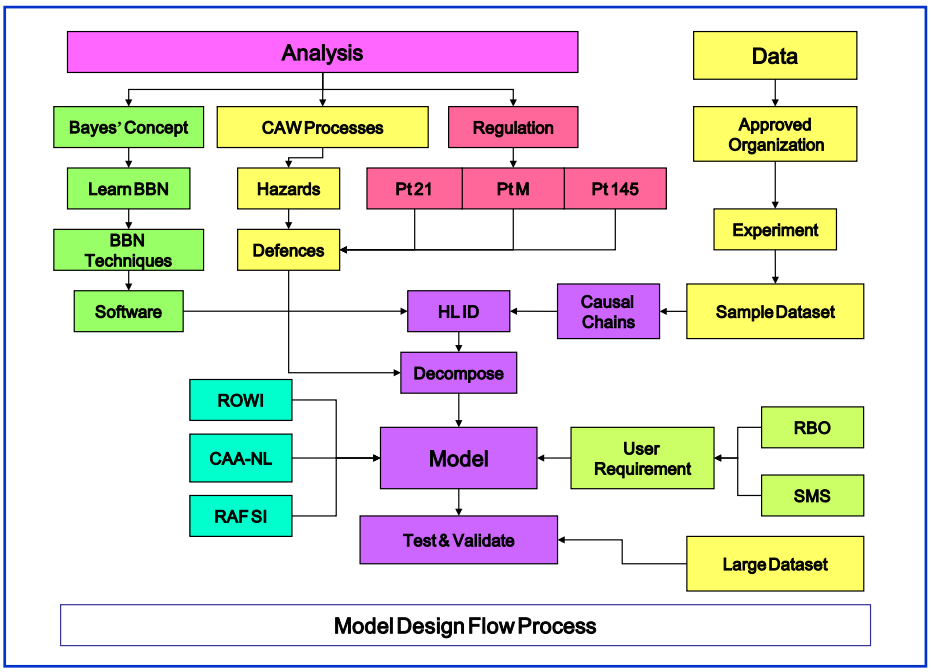


Figure 5.5 - Model design flow process

5.4.1 Learning Bayesian Networks

A fundamental requirement is to gain a good working knowledge of the Bayesian Theory, initially statistics and afterwards its relevance to BBN. At the end of this learning process one should have gained a capability to design a BBN, though at this stage it may not have been advanced to a point that there is a BBN solution to the problem. The solution came later.

Other analytical processes are briefly outlined below.

5.4.2 Analysing CAW processes

- Decomposition of CAW process network identifying relevant approved organizations (AO) and EASA regulations applicable to them.

- Representing risk contribution from each organization in an overall high level Influence Diagram (ID) that represents the problem to be solved.

5.4.3 Relating CAW elements to BBN

- Considering how hazards that exist in CAW processes and defended by regulation could be related to a BBN.

- Considering what data to be used, where they would come from, and having done that, then defining data requirement and setting up data collection process.

- Reconciling differences between root-cause causal chains with what is currently achievable in civil aviation.

As to definition of data, elements of the model were identified and defined as parameters against which data to be collected. Relevant information was researched through literature survey, canvassing subject expert opinion, and complemented with the researcher's prior knowledge and professional experience in this subject.

Figure 5.6 outlines broad areas from which parameters for the model were selected. The flowing arrows represent the matrix structure where hazards and risks, their causal factors exist through the organization, engineering practices, and workface. In order to comply with regulation, the process should be defended against hazards; if the defences either succeed or fail there would be consequences.

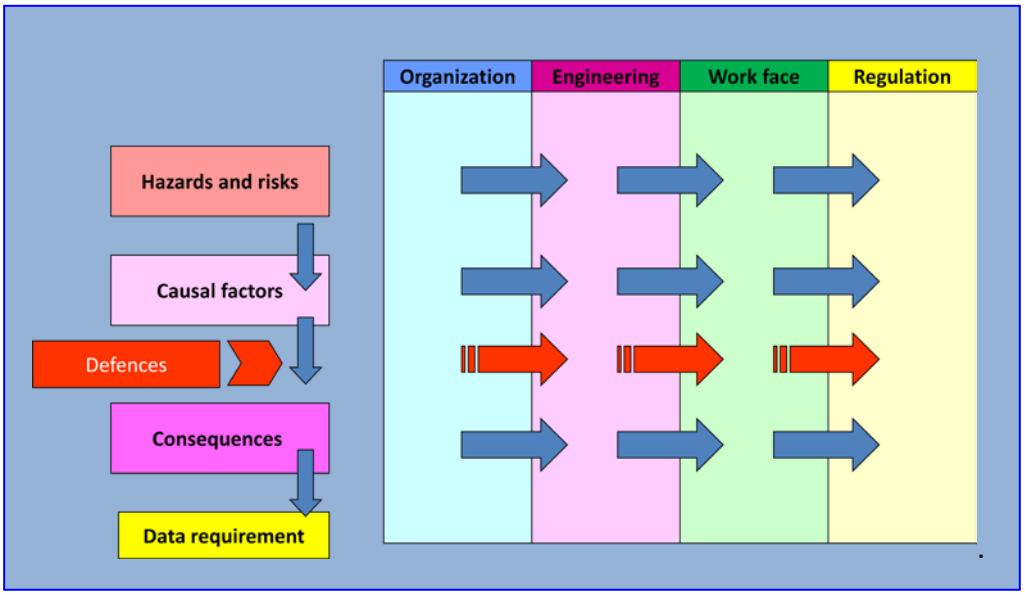


Figure 5.6 – Types of data contributing to the model design

At a much detailed level, the model designer must obtain knowledge of hazards and risks that exist at all levels of CAW processes as well as in associated external entities that provide logistic support to the operators. Details are required of causal factors for human error, contributing factors, interventions and consequences. These are the main data requirements. Simply, information that defines the conditionality of an error or non error event and its outcome constituted the data.

But the data cannot be meaningfully utilized, or organized without a detailed knowledge of their relationship to all other factors, as represented in Figure 5.5 at intermediate level. The required knowledge can best be gained by experience. Otherwise a researcher would have to resort to canvassing the support of a subject expert who is familiar with research work, so that he has the patience and curiosity to harmonize with the researchers objectives. Luxhoj[83, 84] too had recommended that a researcher who is unfamiliar with the subject should obtain a subject expert's technical support before and during the data gathering stage and its interpretation.

5.4.4 Design and construction of a model

This phase involved the following activities, details of which will be described in Chapter Six:

- Reviewing user requirement, e.g. wish-list criteria, and determining how the model could be designed to satisfy user needs.

- Reviewing other relevant risk assessment methods in order to learn lessons (or patterns) from them.

- Synthesizing information from the overall net to design a model.

5.4.5 Test and validation

Once the model was designed, then it should be loaded with data for testing and validation, Figure 5.7. Figure 5.6 already indicated that data may be gathered according to a pre-determined structure, and would come from industry. If data is not available, then the researcher might have to redefine data requirement.

An alternative form is to simulate the data but, to do this, one needs prior information on types of errors and error occurrence profile, not necessarily with precession but in broad terms. The model should be tested with data to confirm that it could be uploaded and compiled, to confirm that the model can accept data without any hindrances.

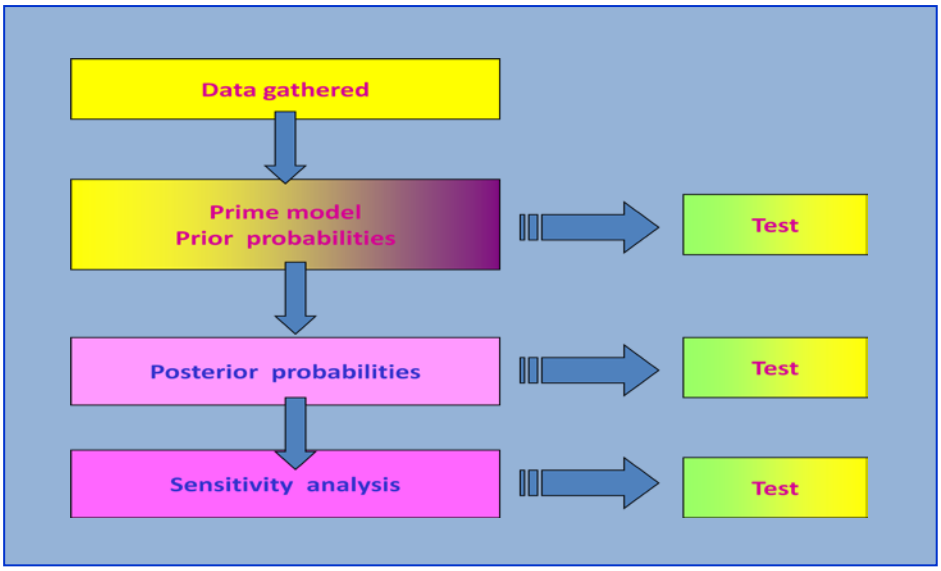


Figure 5.7 – Advance phases of the project

A primed model yields prior probability of error, which can be updated with new information to obtain posterior probabilities. Sensitivity analysis could be conducted on the model to obtain further information on the behaviour traits of organizations. As part of the model design and verification process, the model should be tested at these progressive stages, before declaring the model as successful. This concludes the high-level and intermediate level perception of the methodology.

5.5 A final word on the design methodology

The eventual design for the model was a heuristic solution, i.e. one that evolved through a process of numerous trials to represent all the foregoing factors in one design. There was no reference standard to quote that could be emulated for this part of the design process. In fact it will be seen in Chapter 6 on Model Design that authorities of this topic, BBN for Decision Analysis, such as Clemen[85] has acknowledged that there is no standard guide to the arriving at a BBN solution to a problem, though there are certain disciplines that need to be satisfied in justifying the solution. This is because every problem is unique, and naturally there could well be more than one possible solution to a problem.

In this research study, the main challenge was how to represent the CAW process to derive a risk, and then how the entire phenomenon could be related to a BBN. This was based on vision on how they work together, not gained first time, or on a particular day. It was the outcome of contemplation on various ideas unsuccessfully, and then suddenly one's vision penetrates through the problem and one sees dawn rising through the darkness. Then one realizes that the problem has been solved. Thus the solution is part the result of experimentation with different ideas, part

intuition but the vision of an integrated model attributed to contemplation over the problem.

5.6 Bayesian learning

As one of the underpinning concept for the methodology, the remainder of this chapter is dedicated to establishing the relevancy of Bayesian Belief Networks to safety risk. Comprehension of this relationship is in itself part comprehending the methodology for the design of the model.

5.6.1 Fundamental problem to be resolved

The fundamental question was "how could one predict the chance of an incident occurring due to the presence of several inter-related process errors in a complex system?"

The relationship between errors and incidents has been postulated by James Reason[86, 87] utilizing the "Swiss-Cheese" model to demonstrate how system error could occur. The model illustrates that if multiple errors lined up and critical defences failed to cut in on time, then the integrity of the overall system could be undermined and the system could fail.

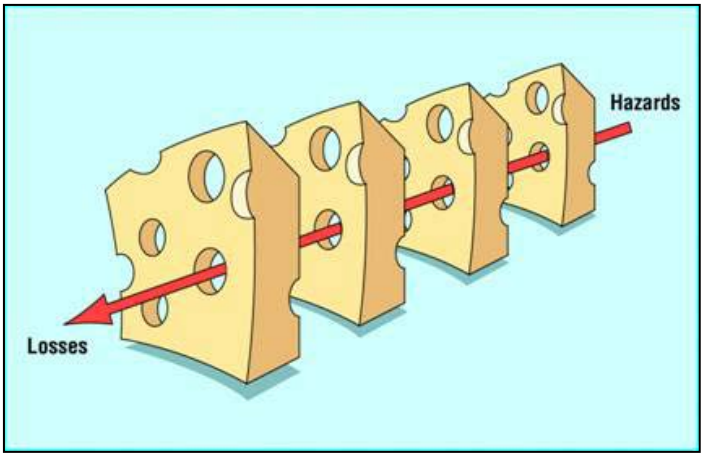


Figure 5.8 – Errors line-up in Swiss-Cheese analogy

The CAW process with inherent errors is analogous to a Swiss-Cheese with holes, where exposed holes represent active errors and hidden holes represent dormant or latent errors. Usually the CAW process performs satisfactorily as it was intended according to Regulation, as people that operate this system adhere to industry best practices, providing its robustness. Yet, following the natural human trait of making

occasional mistakes, errors and omissions do occur in the process system as relatively rare but unpredictable occurrences.

Safety factors built into the design of an aircraft tolerate these errors to some extent. In addition, recognizing the possibility of error, specific defences have been built into a CAW process, which hopefully would recognize an upstream error and correct it before it or its effects migrate through the system and transferred to the end product. It is the industry best practices, safety factors and defences built into the process that prevent accidents.

Occasionally however, defences get omitted, ignored, removed or overridden by people who operate or manage the system. Alternatively, it may be that a defence had not been provided due to limitation of knowledge at the time or the need for defence was overlooked despite what was thought to be thorough planning. Given these conditions, if errors lined up, a hazard could penetrate the system that would undermine the integrity of the end product.

5.7 Bayesian Theory

The above analogy enables us to pose a question as a statistical enquiry, i.e. "What is the statistical probability of one or more errors lining up to cause an incident or, if not, to undermine the integrity of the overall system?"

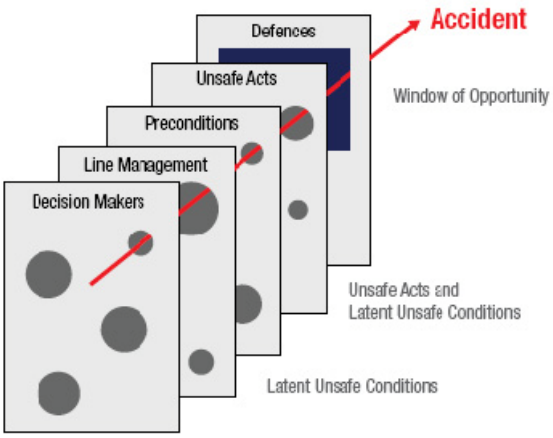


Figure 5.9 – Errors line-up in Swiss-Cheese analogy
(Source: Canadian Transportation Board)

This study considered the possibility that the statistical explanation to the analogy of Swiss-Cheese might be rooted in the Bayesian Statistical Theory of conditional probability[80, 88].

Assume that two cheeses slices represent two sequential layers, A and B (e.g. error in line management and an unsafe act – see Figure 5.9) of activities in a process system and the open and hidden holes representing visible and dormant errors present at these layers. Now consider the probabilities of these respective errors being present, and the probability of them lining up. Line up can occur if error in layer B moves to a certain position given error in layer A has already got there; this incorporates conditionality.

Given two errors with different probabilities P(A) and P(B) occurring independently in a system, it is possible to predict the probability of both occurring simultaneously, as:

$$P(A \text{ and } B) = P(A) \times P(B) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad 5.1$$

P(A) and P(B) being independent are called “marginal probabilities”.

In an incident resulting from a system error, error sequence may occur in 2 stages. First error A occurs, and given A had occurred then error B occurs. Both error A and error B must be present for the incident to occur, but conditional upon one occurring first. The probability of A and B occurring together in the sequence with this condition is:

$$P(A \text{ and } B) = P(A) \times P(B \mid A) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad 5.2$$

P(B l A) is the “conditional probability” of B occurring, in this case, given A had occurred.

Within the system A and B together could also occur in different ways, namely B first, and then A. Then,

$$P(A \text{ and } B) = P(B) \times P(A \mid B) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad 5.3$$

Since P(A and B) is the same in each case (Equations 5.2 and 5.3) could be rewritten as follows:

$$P(A) \times P(B \mid A) = P(B) \times P(A \mid B) \quad \ldots\ldots\ldots\ldots \quad 5.4$$

from which a formula could be derived:

$$P(A \mid B) = [P(A) \times P(B \mid A)] / P(B) \quad \ldots\ldots\ldots\ldots \quad 5.5$$

This expression could be represented in the following network at Figure 5.10, given two prior conditions and a new posterior condition.

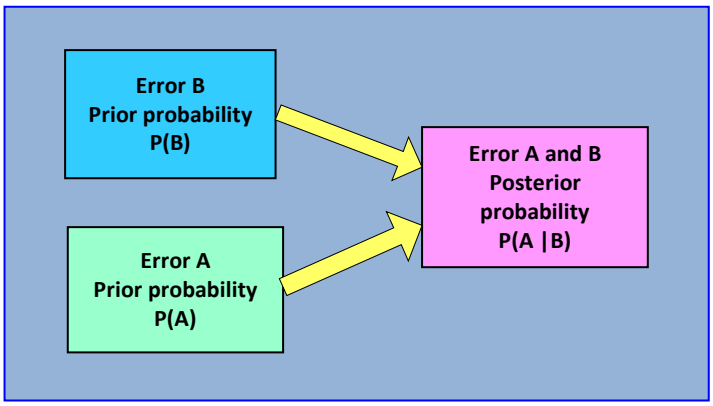


Figure 5.10 – Conditional probability – Single element

In a process system, this could be equated to a probability of errors occurring independently in an Event A in one part of the system, and an error occurring independently in another Event B in another part of the same system. The independent marginal probabilities are called "prior probabilities".

If within the system, Event B influences Event A through their interconnectivity, then a dependency has been set in the overall process. The error probability at the outcome of the interconnectivity can be computed as P(A I B) which is interpreted as the probability of error A given error B. This conditional probability is called "posterior probability".

This joint error probability is in fact the probability that the two errors from A and B could line up causing a system weakness.

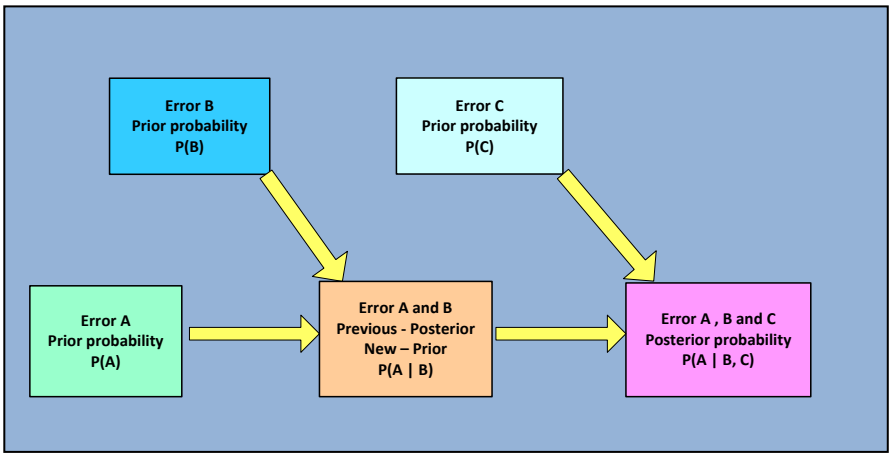


Figure 5.11 – Conditional probability – Multiple elements

If the process network has multiple interconnected tasks, then the error probability at each downstream node could be thus evaluated using this method. The upstream

posterior probability becomes a new prior probability, and the downstream node becomes the new posterior. Figure 5.11 illustrates this new situation.

In a complex network, the pattern could be repeated until all events that need to be taken into account are exhausted. Thus in a chain of events containing errors, the probability of error at the most downstream node represents the aggregate conditional probability of error of the interconnected network of events.

The aggregate probability of error, in this 3 events chain of A, B and C then becomes:

$$P(A \mid B, C) = [P(C \mid A, B) \times P(A \mid B)] / P(C \mid B) \quad \ldots\ldots\ldots\ldots\ldots \quad 5.6$$

- P(A I B, C) is probability of error in A given error in B and error in C had occurred.
- P(C I A, B) is probability of error in C, given error in A and error in B, i.e. this being the same as probability at the interconnecting node between A and B, i.e. P(A|B).
- P(A I B) is the new prior probability, whereas it was the previous (upstream) posterior probability.
- P(C I B) is the probability of error C occurring, given error in B.

Even though there is no direct connection between C and B, their relationship exists through the terminating node to which C feeds in as well as B feeds in via the previous posterior.

This relationship could be repeated for a continuous chain of events, which can be extended as new information (or new events) becomes available.

Returning to Equation 5.5 above, conditional probability calculated with this formula is somewhat biased when it is applied to a selected sample of events A and B where errors were known to have occurred. The bias is there, because error in event B could be associated with other events which are “NOT A” and these have not been accounted for. Therefore to remove this bias, the probability of error occurring in event B should be related to the whole population of events in a group which are both “A” events and “NOT A” events.

An example of such a situation is given in Figure 5.12.

A surveyor wishes to determine the significance of “Document Error “on incidents that occur in his organization. As error events and incidents are monitored at this operator, the surveyor takes the statistics for failed sectors and determines how many of those sectors have had human error due to document error.

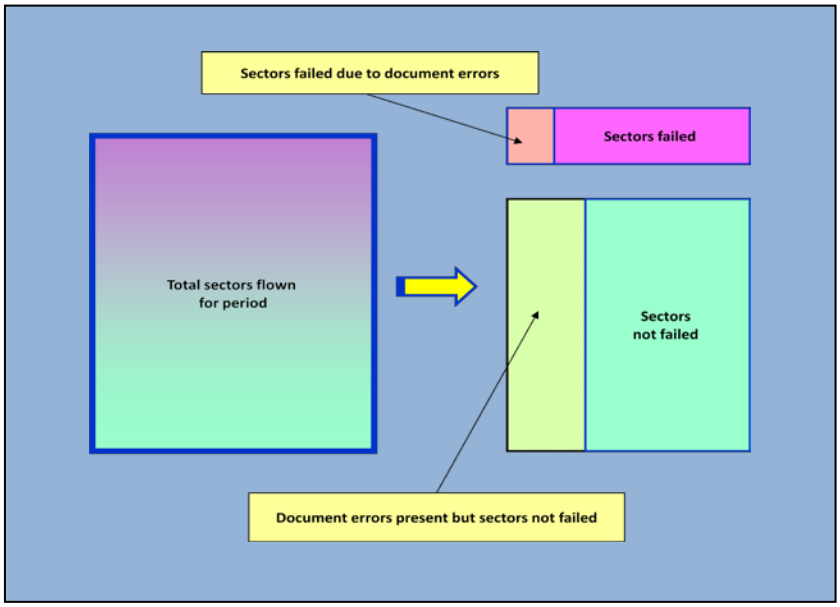


Figure 5.12 – Removing bias by accounting for all similar errors

Given these data, if he makes an estimate based on incident data only, then he would be making an unfair estimate of the probability of "Document Error" contributing to incidents in the operator's fleet. This is because there could well have been Document Errors induced human error in some of the other sectors flown that had not failed. Therefore to make a fairer estimate, he should take into account other sectors that had not failed, in which "Document Error" induced human errors were known to have occurred yet the sector had not failed.

The following analytical approach to the probability calculation ensures that bias is eliminated. In this example:

- P(B) = Marginal probability of Document Error
- P(B|A) = Probability of document error, given probability that Sectors had Failed.
- P (A) = Probability of Sector Failed.
- P(B|Not A) = Probability of Document Error, given Sectors had Not failed.
- P(Not A) = Probability of Sectors not failed

In order to perform the correct calculation the previous expression for the term P(B) has been modified to give:

$$P(B) = [P(B \text{ I } A) \times P(A)] + [P(B \text{ I Not } A) \times P(\text{Not } A)] \quad \ldots\ldots\ldots\ldots\ldots \quad 5.7$$

This is the probability of error B occurring in the whole population, i.e. the sum of probability of error B occurring in those events A where there are errors, and the probability of error B occurring in events other than A. If "A" represents Sectors Failed, then "Not A", Sectors Not Failed.

Although the "Not A" events may have a relevance to B events (i.e. Document Errors) either on its own or by lining up with another error, "Document Errors" in this proportion of sectors had not led into any incidents. This point should be borne in mind when considering data from a practical environment, which will be input to an eventual model.

Equation 5.5 can now be re-written to represent the unbiased situation.

$$P(A \text{ I } B) = [P(B \text{ I } A) \times P(A)] / [P(B \text{ I } A) \times P(A)] + [P(B \text{ I Not } A) \times P(\text{Not } A)] \ldots\ldots\ldots \quad 5.8$$

The denominator contains the sum of two probabilities, these being the joint probability P(B and A) plus the joint probability P(B and Not A). It can be seen that P(B and A) is in fact the numerator of the right hand part of the original Equation 5.5.

Thus the left hand side of the equation which is P(A given probability B) is the ratio of joint probability P(B and A) divided by the sum of joint probabilities of (B and A) and (B and Not A).

Similarly, Equation 5.6 can be re-written as:

$$P(A \text{ I } B, C) = [P(C \text{ I } A,B) \times P(P(A \text{ I } B)]/ [P(C \text{ I } A,B) \times P(A \text{ I } B)] + [P(C \text{ I Not } A, B) \times P(\text{Not } A \text{ I } B)] \ldots 5.9$$

It follows from there, that the generic equation for probability A of a series of mutually exclusive events, B1, B2, B3.... Bn, (i = 1 to n), can be written as:

$$P(A) = \sum_{i=1}^{n} P(A|Bi).P(Bi) \ldots\ldots\ldots\ldots\ldots\ldots 5.10$$

The derivation of the formula appears to make this analysis un-necessarily complicated, when it is quite simple to estimate P(B) from the base data, simply by putting numbers and undertaking a manual calculation. In fact, that is so, but if the manual calculation had to be done several thousand times, even millions, as it would be required in an industrial process setting, then it would not be efficient to do it manually. The simple analysis explains how to derive the formula that could be used in a computer program later.

Now, returning to the relevance of Bayes' theorem to the phenomenon of alignment of errors, the statistical expression (Equation 5.8) could be better visualized with a Venn- Diagram given in Figure 5.13. The Venn diagram is similar to stacking slices of Swiss cheese to see which holes line up.

In Figure 5.13 where the P(AIB) is the size of the intersection of the 2-subsets Event A Sectors Failed and Event B Document Errors, expressed as probability, i.e. the probability of Document Errors featuring in Sectors that Failed. The outer ellipse represents the total population subject to the survey: i.e. All sectors flown where

some sectors had errors and failed, while a larger proportion might have had errors but not failed. Of those Not Failed, some had Document Errors, but did not make Sectors Fail.

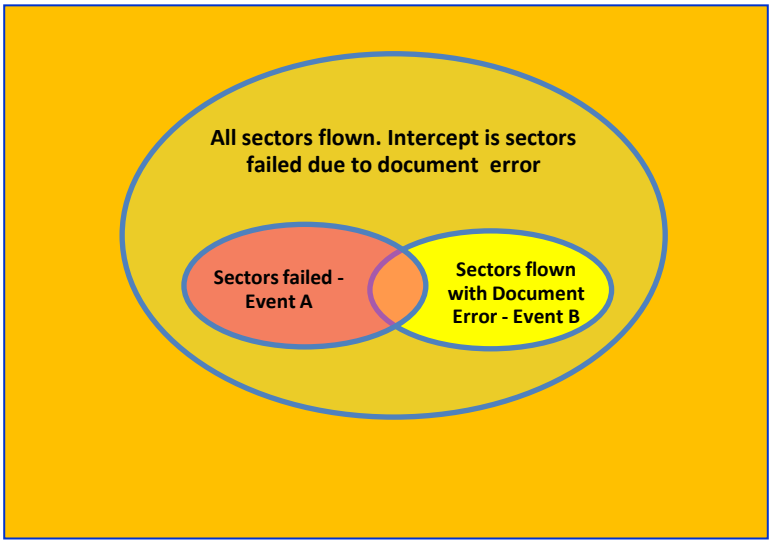


Figure 5.13 - Venn diagram of Event A and Event B

Although the mathematics and visualization turned out to be relatively simple up to this point, in real life conditions the situation is more complicated.

For example, a network representing CAW process could contain several scores of nodes simulating significant events of the process, depending on the resolution required. Moreover, each event (or node) may contain several causal factors or if not management information.

In reality, Event A (Sectors Failed) could have been caused by more than one type of human error, attributed to different causal factors, thus giving an error distribution. This is similar to the cheese slice having X1 number of holes of diameter D1, X2 holes of diameter D2 etc until Xn holes of diameter Dn. The same situation would apply to Event B. The problem that has to be solved then becomes extremely complicated: which type of error in Event A would line up with, what other type of error in Event B, and Event C and so on, and what is the probability of that occurring?

It follows from the foregoing that the CAW process could be represented as a series of multivariate probability distribution curves, each simulating a different event. Such a family of curves could define one set for prior conditions, and another set define the posterior in response to a new input, given there was a prior distribution. This type distribution is known as Dirichlet Distribution[80, 89] which being three-dimensional resembles a “hay stack”.

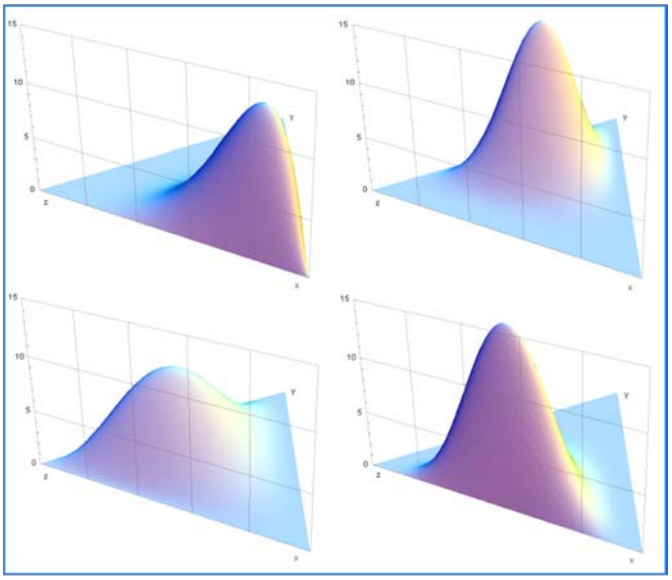


Figure 5.14 – Dirichlet distribution
(Source: en-image:Dirichlet_distributions.png - Wikipedia)

Figure 5.14 is an example of a set of different probability distributions of Dirichlet's form. Relating to a Bayesian Net, X-Y axes define the State of Nature and Probability Density of variables respectively and Z axis define the variation of events (or different nodes). The sharpness of the peaks indicate where the mass of the distribution is concentrated, sharper the peak, greater the concentration. Distribution of priors from a large sample size/ population tends to display sharper peaks, whereas small sample sizes/population returns a flat distribution.

This research study has not gone into an analysis of advanced statistical theories on which the current knowledge of Bayesian Theory is based, and instead focused on the application of the concept through Bayesian Belief Networks, this being the main objective of this research program.

5.8 Handling Bayesian Formula in practice

Returning to the formula derived above, if 5 events each containing 20 potential error sources simultaneously interact with another sixth event (i.e. in parallel), then they could generate 20^5 = 3.2M combinations for which conditional probabilities would have to be calculated. The formula can get very complicated indeed, the amount of computation, organizing and storing the data manually becomes humanly impractical. Such work is best suited to a computer. Invariably a computer would have to be used together with appropriate software. Commercial off-the-shelf software packages are available that could do this work.

The demonstration at Fig 5.12 also underscores an apparent weakness in expert systems based on experience. That is, there is a general tendency amongst experts to remember and bring forward failures and to ignore situations where errors might have happened and successfully defended.

It is quite understandable if an expert is cautious in his subjective judgment but, in fairness, due credit should be given to a defended system where errors might have been detected and defended. This is one reason that all data from one-organization should be examined in determining risk, and that data should represent both error incidences and non-error performance. Obviously this example highlights the advantage of maintaining records of errors and sectors flown even if the error did not fail the sector, as it is generally known in the profession for defended system.

5.9 Bayesian Belief Network

Given that a CAW process system may contain several hundred events, the entire process may be represented by a complex network where the configuration of nodes similar to those in Figures 5.10 and Figure 5.11 may constitue the primary elements. The nodes are assembled in a rationale manner; the causal chain has a direction indicated by linked arrows, and its nodes have a sequence, and a relevance or relationship according to their functionality. However the path cannot have feed-back loops, making this network a directed acyclic graph (DAG).

Embedded within the nodes in the network are descriptive and statistical information on the event and its states of nature. Such a network of nodes that has been uploaded with statistical data then becomes a BBN. With the mathematical manipulation of information contained in these networks, it may be possible to infer other “what-if” information on the behaviour of the overall process, or to interrogate what would happen at other nodes that represent upstream or downstream events.

The design of BBN will be discussed in detail in Chapter Six. At this point a simple introduction and prcatical use of a BBN is made.

5.10 BBN commerical software packages

Commercial BBN software packages are available which faciliate the design of a BBN and undertake the computation of probabilities as well as numerous other associated tasks.

Two different software packages were considered for this study, NETICA and Genie and Smile.

NETICA is marketed by NORSYS Corporation of Canada, and is commercially supported. The other system GENIE & SMILE has been produced by Decision Systems Laboratory of Pittsburgh University, USA. The latter has no commercial support arrangement, though it is supported by a "blog-based" website. Genie is understood to be more user-friendly and has more features to improve its presentation capability.

However based on feedback from other user experience, certain desirable technical features, low cost and reliable support, NETICA was selected. NETICA's scope and full range of capabilities could be found in NETICA User's Guide[90].

5.11 BBN worked example using NETICA software

Although NETICA is a known, well proven and widely used commercial software package, being commercially confidential proprietary material, its algorithm and computer codes were not available to the customer. Therefore some test runs were done to gain confidence on if the program returned the same results as that is obtainable from manual calculations. One of the tests is described below.

5.11.1 Setting

A BBN was drawn up to represent a simple 2-part maintenance activity: an inspection and a follow up defence, i.e. an independent oversight of the maintenance task.

Results from 10 separate operations were uploaded and compiled in to the network, to obtain prior probabilities at each node of the network. Later the network was used to conduct inferences, i.e. predictions, given set evidence at selected variable parameters, together with recording of responses at other parameters, e.g. probability of error at the outcome for a given set of conditions. Each of these conditions can be regarded as evidence of posterior probabilities in response to new inputs, given prior conditions.

Response values were then examined to see if they fit in with the predicted values using Bayes' Formula, manually.

The test cases were run and the results matched the figures obtained long-hand, confirming that NETICA software is a good representation of the calculations from first principles. This produced a satisfactory result. Details of the demonstration and manual calculations are presented below.

5.11.2 Details

In this simple BBN, say,

- Event A is an inspection which either contains either an Error or No Error.

- Let Event B be a defensive inspection that turns out to have either an Error or No Error.

- Outcome could have either a Joint Error or No Error.

That is if the inspection at Event A fails (i.e. has an Error) and the defensive inspection at Event B also fails (i.e. has an Error), then there is a Joint Error at Outcome. There are 10 separate inspections and 10 separate defensive inspections following the initial inspection.

5.11.3 Problem to solve

Given these prior conditions, what is the probability of Joint Error at Outcome for the prior conditions, and then, determine what the Joint Error at Outcome is, if the next inspection produces an Error at Event A?

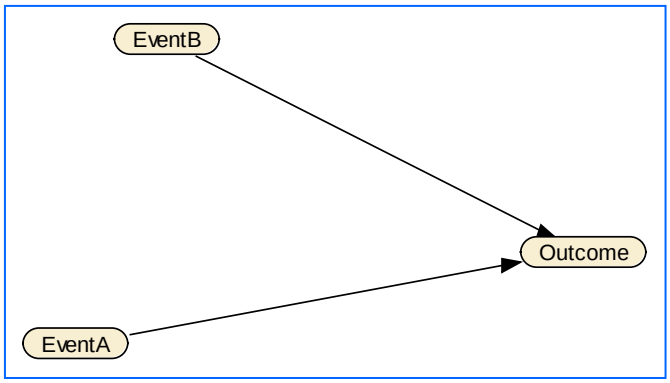


Figure 5.15 – Simple BBN

5.11.4 Explanation

In this example, what is being simulated is the integrity of the maintenance process, i.e. how accurately people are doing their work without making mistakes, i.e. the reliability of the human in undertaking the CAW process satisfactorily. The process has been set on the assumption that there could be a defect in the system, e.g. a fault in the latch of the cargo door and that the first inspection could be confirmed erroneous or error-free by a second independent inspection or by the functioning of a sensor that gives a remote indication in the cockpit .

An engineer inspects the latch, this is Event A, and later another engineer, say, a supervisor, rechecks the work of the first for the integrity of his work, i.e. Event B that one could refer to as Defence.

Take the Inspection (Event A). The engineer may do the task correctly and discover a fault. In this case No Error was committed on the inspection because he did it properly. If there was no fault with the latch, we take it also as No Error regardless of the fact the inspection was done properly or not (we cannot fault the engineer without evidence). However if there was a fault with the latch, but not detected because the inspection was not thorough, then it is recorded as Error.

Now coming to Event B which is the Defence (against potential error in Event A), this is usually a second, independent check of the critical parts of the previous inspection by another person, to make sure the first inspection was done properly.

Again, if Event B was carried out properly and if there was No Error at Event A, then Event B should return a No Error. However if Event B was not done properly, then Event B returns an Error regardless of Event A was at No Error or Error. As before, if there was no fault at the latch in reality but none of the inspections was done properly then the system is still good (due to system's design reliability) but we have to accept that Event B is returning a No Error.

In the 3rd node, Outcome, this indicates the outcome of two different inspections on the same critical component, done successively (or if we are assuming the cockpit indication, the defence action may be done either concurrently or consecutively).

The Outcome returns No Error:

- If there is no fault in the system, or
- If Event A and Event B was properly done (Event A No Error and Event B No Error)
- If Event A was done properly but Event B was not done properly (the latter is redundant if Event A was done properly).
- If Event A was not done properly (Error) and Event B (No Error) was done properly (because the fault was captured in the defence).

However the Outcome returns Joint Error:

- If Event A was not done properly (i.e. Error) and Event B was not done properly (i.e. Error). This is a maintenance process system failure.

5.11.5 Observed Data

Table 5.2 represents the observed data.

ID Number	Inspection (Event A)	Defence (Event B)	Outcome
1	No Error	No Error	No Error
2	No Error	Error	No Error
3	Error	Error	Joint Error
4	No Error	No Error	No Error
5	No Error	No Error	No Error
6	Error	No Error	No Error
7	Error	Error	Joint Error
8	No Error	No Error	No Error
9	No Error	No Error	No Error
10	Error	No Error	No Error

Table 5.2 – Observations

5.11.6 Data file

A NETICA compatible text file was produced using the information in Table 5.2.

5.11.7 Compiled BBN

Data was then uploaded into the network through a custom-design data file compatible with the program, and the network was compiled to generate a BBN that gives prior conditions.

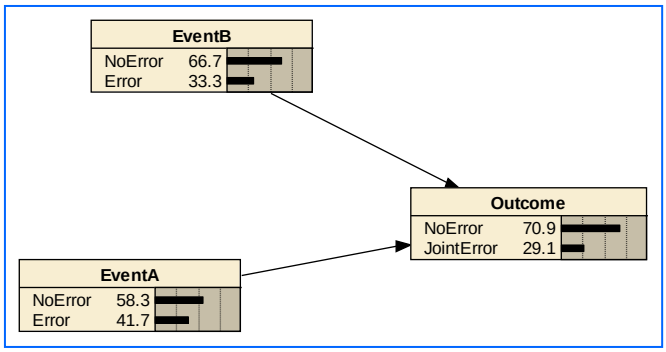


Figure 5.16 – Belief bars on compiling the net

NETICA program returned the belief bars at each node as shown, Fig 5.16. These represented the distribution probability of each state of nature at the node, taking into account the pattern of arising and observations from the sample.

5.11.8 Inference

Now, evidence was placed at relevant nodes (instantiated) to represent the following conditions and the BBN returned different outcome, Figures 5.17 to 5.19.

Evidence if Event A = Error and Event B = Error

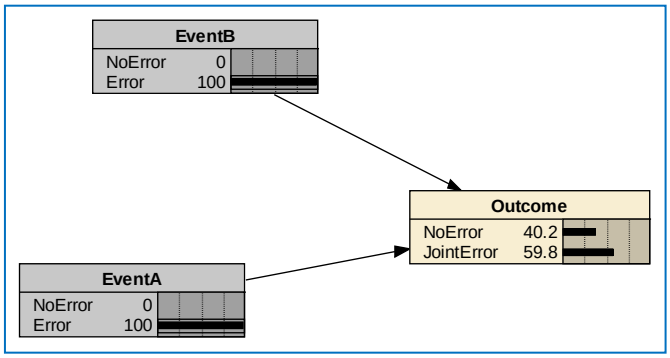


Figure 5.17 – Evidence at A = Error B = Error

Evidence that Event A = Error and Event B = No Error

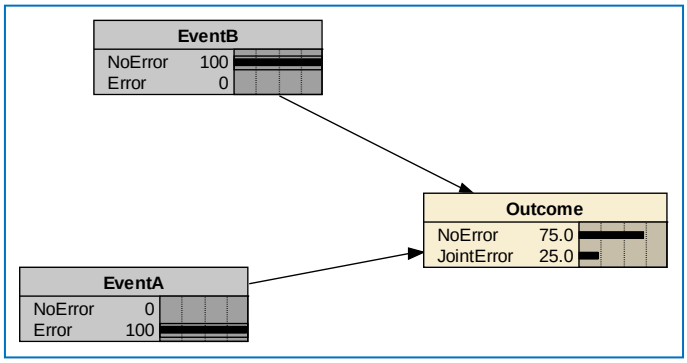


Figure 5.18 - Evidence at A = Error and B = No Error

Evidence that Event A = Error given prior conditions

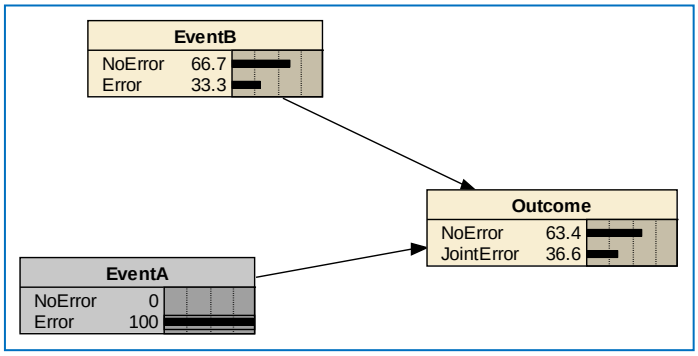


Figure 5.19 - Evidence at A = Error and B = Prior conditions

5.11.9 Mathematical calculation

In the network, Event A and Event B are independent (assuming Outcome is not observed). In that case, from the definition of independence, we can conclude that:

P(A|B)*P(B) = P(B|A)*P(A) = P(A)*P(B), so
P(A|B) = P(A) and P(B|A) = P(B)

Question: What is the probability of error at Outcome, if the next inspection (Event A) produces an Error?

Probability at Outcome is P(O); O is Outcome.

This is calculated directly from the network, see belief bars. Use the numbers from network directly, having set the Nodes to the conditions below.

P(O=JointError|A=a, B=b) – this is just a number from the conditional probability distribution of node Outcome, depending on instantiations Node A = a, and Node B = b.

For example, A=Error and B=Error: P(O) is 0.5976071. See Fig 5.17.

P(O=JointError|A=Error) = P(O=JointError|A=Error,B=Error)*P(B=Error) +
P(O=JointError|A=Error,B=NoError)*P(B=NoError)
From the net,
P(O=JointError|A=Error) **= (0.5976071*0.333333) + (0.25 * 0.6666667) = 0.36586901**

The rounded up values are shown in Fig 5.17, Fig 5.16, Fig 5.18 and Fig 5.16 respectively. Exact figures obtained from the

This value is approximately **36.6%** the figure given in the node "Outcome" against JointError.

5.12 Summary of Bayesian learning

Summarizing the application of Bayesian concept to the research objective, it became clear that the statistical solution to the Swiss cheese model is the key to finding a risk assessment model. Experimentation with a simple BBN has demonstrated that the concept could be utilised to compute the statistical conditional probability of a system error occurring in a process. This small element of BBN would then become the fundamental building block for a complex process network.

5.13 Data requirement and collection

Regarding data, two factors had to be considered at the outset: Type of Data required and the Method of Collection.

5.13.1 Type of data

Specific data to be gathered will be defined in Chapter Six, Design of the Model, and in Chapter Seven, Working with Data. In general data requirements fall into two categories:

- Quantitative data on error incidents, consequences, and supporting information such as aircraft utilizations; these may be either processed statistical data or unprocessed raw data

- Qualitative descriptive data on errors and incidents, together with information on CAW processes, rules and regulation, environment of operation and conditions, methods and culture, best practices, experiences, expert and individual opinions.

5.13.2 Method of collection

Data gathering will be through literature research, by accessing existing relevant databases of the Authority as well as from Approved Organizations who might be willing to participate, and from other stakeholder organizations such as CHIRP, IATA, ICAO and learned bodies who might assist. Furthermore, qualitative information could be obtained from interviews and content analysis of case histories.

Interview techniques in particular were found to be very successful from the point of view of clarity and data quality; they also help to promoting the study amongst stakeholders and canvassing their support.

Multiple methods when applied selectively would yield data more effectively on the basis of what data is required and how best to get it on time. It is a recognized technique and has been successfully used before in a research study by RAND Institute into the role of personnel in NTSB aviation accident investigation[115].

5.13.3 Alternative methods

Alternative methods considered were simulated experiments of maintenance error occurrences and their outcome, and questionnaires to licensed engineers and managers about error situations.

Simulation of error situations under controlled experimental conditions were considered but dismissed as impractical or misleading for a number of reasons. People would not behave naturally in simulated conditions if their behaviour that was being monitored. Sense of self-protection, dislike to be judged by others on personal traits, and even deliberate acts to spoil the result are natural hindrances to achieving a reliable result from simulated exercises. Despite these limitations, it is known that simulation is widely used under exercise conditions, training or evaluation of a process, where the individuals have to perform as part of their training. On such conditions the participants themselves are most likely to derive a benefit, which in turn makes the simulation worthwhile for them, thus securing their cooperation.

Simulation was also impractical in a busy aircraft maintenance area where safety and cost issues were finely balanced. Managers would not have permitted data gathering in an environment where industrial safety is critical, distraction of workers from primary work could risk compromising the safety of aircraft, and labour costs and diversions are highly sensitive issues. Therefore, simulation or even the alternative idea of observing people at work was ruled out.

Questionnaires are alternative forms of data collection but it was not suitable on this occasion. This study has primarily focused on hard facts of events occurred rather than people's opinions or about their individual judgments or personal experiences. In an industry where the free flow of information is highly controlled and pressures on employees' job security are real, questionnaires would have yielded correct information.

Intentionally Blank

Chapter Six

Model design

6.1 Influence diagram preceding the model

This Chapter describes the design of the model in progressive stages and how the model evolved from an influence diagram (ID). There was no known literature that provides a precedent to the detail design of a model of this scope as envisaged in this research study. Therefore design was attempted from first principles, and as explained in the following sections. The flow diagram at Figure 6.1, which was drawn up retrospectively on the basis of the experience gained, is produced here for the benefit future researchers.

The modelling process started with the setting out of an ID. An ID is a graphical way of representing a decision problem. Graphically the ID resembles a neural network of variables represented as nodes, and their inter-nodal relationship represented as links. Such a network is technically defined as a "Directed Acyclic Graph (DAG)"; it is a graphical representation that has an identified direction, either forward or backward, hence called "directed". It is "acyclic" because it should have no feedback loops.

The first consideration in setting up an ID is the clarification of the decision problem, i.e., "What decision problem the ID should represent?" Further the designer should identify and display the essential elements that influence the decision and the way they are inter-related. According to Clemen (2000)[85] four contributory factors must be considered in this regard. These are:

a. End product (or the output) from the model.

b. Technical logic.

c. Architecture, i.e. its components, their sequence and relevance

d. Data intended.

These factors are analyzed in the following sections.

6.2 Output from the model

The expected output from the study is a methodology for assessing and quantifying risk, which could be used in two industrial applications, i.e. in support of Safety Management Systems (SMS) and Risk Based Oversight (RBO) concept.

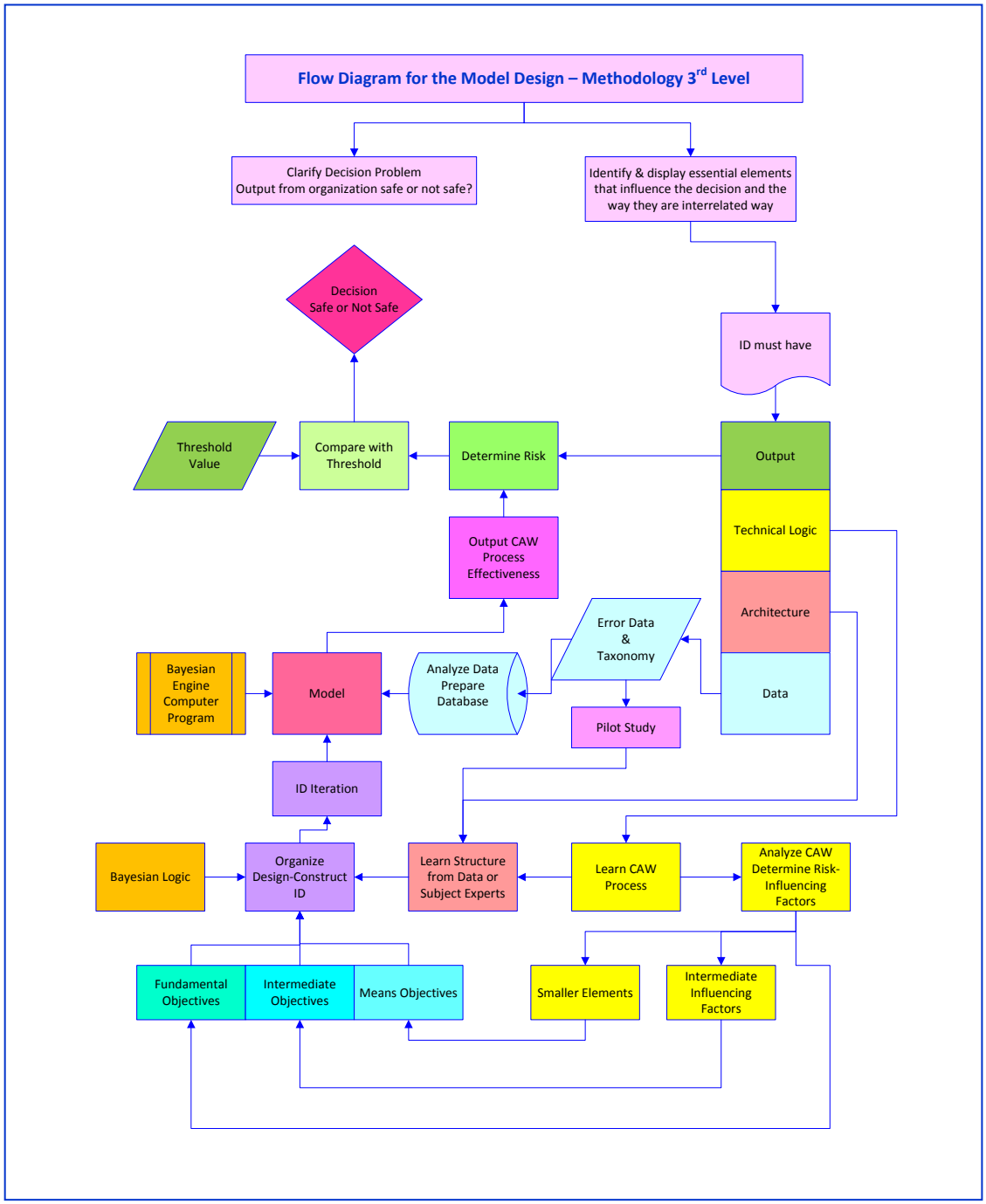


Figure 6.1 – Flow Diagram for Model Design

SMS focuses on the ability of an organization to perform safely in all its activities. One component of the SMS is the assessment of risk arising from consequences of hazards that exist in the organization, infrastructure and processes. This study examines just one area that contributes to flight safety risk, i.e. risk contribution from human error in the CAW process and its organization. It follows therefore, the decision problem to

which a solution being sought is, “The organization and its CAW process activities, do they pose a safety risk?” The answer may be either an affirmative or a negative. Thus the problem to be solved in relation to the model is “How to configure a BBN to represent the CAW organization and processes in order to derive an either Yes or No answer on risk? “

Regarding flight safety, an organization or a process can be only either safe or unsafe; the states are mutually exclusive. There is no intermediate state between safe and unsafe. However safety can be conditional. Perception of safety can vary between people or between stakeholders, according to the threshold of risk agreed between the parties concerned or specified by higher authority. That is, given certain conditions, if the risk is greater than a previously agreed threshold then it may be unsafe; otherwise it may be safe.

The model outputs a risk level that could be compared with an agreed threshold. At present there is no such agreed quantitative threshold for CAW processes. If such a threshold could be set up using this methodology is an open question, which this thesis will try to address later in the thesis (Chapter Nine). The risk level is the end product from the model which may be viewed according to the values and objectives of the organization that owns the process that is being modelled, and what the National Aviation Authority (NAA) considers as the safe threshold.

To bring forward material previously learned, as it is now required for the application, risk can be expressed as a single number, this being the product of probability of the hazard and its severity of its consequences. For quantification, it may be necessary to find a common measure for severity. For instance, risk could be the product of: Probability of a hazard occurring x monetary value of its consequence.

Some forms of consequences can be the loss of reputation, personal injury and loss of human life. It is acknowledged that they may be beyond valuation, especially to the victims, and therefore even the idea of putting a monetary value to the loss of life can be seen as abhorrent. But, it is general knowledge that courts do award monetary compensation in settlement of legal claims involving personal injury and death and that actuarial methods exist to determine their monetary value.

Alternatively, risk could be expressed as: the probability of a certain consequence given that there is a probability of error present at the end product from the process, e.g. one-in-million chance of a catastrophic accident occurring, given that there is one-in-hundred thousand chance of a maintenance error being left undetected at release of an aircraft to service. This is an idea that will be proposed in this research study

(Section 6.32) because that form of expression may be more meaningful to the manager than a single non-dimensional number.

6.3 Output from the CAW process

While the output from the model helps to define the decision problem, focus on the output from the CAW process may help to determine the means of solving the decision problem.

The intended end product from the process is the generation of an airworthy aircraft for a revenue earning flight. If this objective can be achieved consistently, then the organization and the process can be considered as safe. But in reality, the end product may turn out to be unsafe sometimes. For example, an LAE might release an aircraft to service believing that it is safe and airworthy on account of it meeting procedural requirements, whereas in reality it might not have been safe because of the presence of a maintenance errors or CAW process error that has been committed and left undetected. A safe outcome would be known only if the aircraft reached its destination without an incident.

Once an aircraft is released to service, its safety depends on flight operations, management of airfield and ATC as well as other extraneous factors such as natural hazards or sabotage. All these other factors could cloud the issue when considering flight safety risk. Therefore, in order to examine only the effects of CAW processes on airworthiness, it is necessary to discount (or shut off) all other external influences acting on a post-Release to Service aircraft by assuming that other than CAW processes, everything else is perfect and error free. This model will thus focus on post-Release to Service aircraft that may be affected by undetected CAW errors only, and the contribution made by the organization's CAW process towards that risk.

That said, it is acknowledged that, often, there are situations where causal factors for CAW errors in fact lie in areas that fall outside the CAW process domain, such as flight operations or human resources. Examples are: the non-procedural practices when rectifying running faults, communication failures at Flight Ops/ Maintenance Control interface, and employment of unqualified personnel. These, as well as similar issues relating to other external factors would be accounted for in the model through appropriate techniques designed into the model.

In regulatory oversights, it is the integrity of the organization itself and its capability to deliver a safe flight consistently that is assessed. In current methods, assessment is based on the organization either complying or failing to comply with set regulations. The proof of compliance is obtained by checking the organization infrastructure,

procedures and individual aircraft's CAW status against regulatory requirements and industry best practices. Since the regulations represent the collective knowledge and disciplines acquired from experience of safe operation of civil aircraft, it is generally assumed that an organization that consistently complies with regulations is safe; those who are non-compliant are considered unsafe at least in those areas that non-compliance was found.

Currently, all organizations and its activities are audited under ICAO guidelines (100% in 2-years) but the number of inspectors allocated to the organization may depend on NAA perceived risk, based on the organization's size of operation and capability, as well as on its performance in audits.

Philip Hampton [PH Report] challenges the cost of administering the regulation this way, recommending research into alternative ways of discharging regulatory responsibilities on the basis of risk. Given that SMS could have a strategic level risk assessment method incorporated into its system, then it might be possible for NAA to utilize the same model output as an indication of the risk from each organization. This model design tries to find a single solution to meet both these needs.

This approach could also help to harness better cooperation from those stakeholders who hold the view that regulatory compliance in itself does not ensure flight safety, and that it is the technical disciplines and alertness of people at the work face that assures safety. The model could test this view; they could use the model either to substantiate their claim or if not to accept that regulatory compliance indeed makes a major contribution to safety.

In this problem, the organization and the processes are intrinsically inseparable. If the delivered aircraft is unsafe or technically non-airworthy, then it also means that the organization is also unsafe in the way it performed. In responding to this question, the ID will return a measure of the degree of uncertainty, this being the risk.

The developed ID would define how this measure is represented. In a strategic situation, it is the general overview of the state of the organization and process (in a general sense) that is represented by the ID, and not the safety of any specific flight. This is because the general state of risk is based on accumulated historical error data. However, it will be shown later that, given a general result as presented in the BBN, it might be possible to draw an inference about the next flight to be launched by the organization in so far as the fidelity of its CAW process is concerned (Chapter Seven).

6.4 Technical logic

Key elements of the CAW process were introduced in Chapter Two. CAW process, the organizations that manage the process, the Regulation and those organizations that manage regulatory compliance oversight are all hierarchical processes or hierarchical organizations. As such the model would also reflect this quality.

A number of approved organizations work collectively to ensure that CAW of an aircraft is maintained. A decision process takes place at different stages of the CAW process, where a judgment is made by authorized specialists or managers about the airworthiness of the aircraft. In practice the judgment is based on the assumption that if relevant parts of the CAW process have been completed satisfactorily on a continuingly airworthy aircraft, then the end product from the process is airworthy, given that there are some checks and balances are in position to substantiate the assumption.

Despite the checks and balances, errors do occur within this system, which go undetected. It is these errors that concern flight safety, as they get migrated forward through the CAW process to the flight. Adverse flight consequences and resulting cost to the organization that delivered an unsafe flight could be serious.

A model that represents the airworthiness decision process should therefore identify all the approved organizations, encompassing tasks and personnel that contribute to generating a safe flight as well as to errors in the CAW process which might risk safety. The model should identify where errors occur within the overall process.

To make it possible, the ID should represent both the hierarchical structure of approved organizations involved with the CAW process, the interfaces through which activities and information flow between the associated AOs, namely, Pt 145, Part M and Part 21 AOs and departments.

The model should identify those interfaces where CAW process or its organization interacts with other non-CAW support services such as human resources or operations such as flight operations. Similarly, the model should differentiate between the technical sides of the business from the commercial side and identify the points where there is a handshake between the sides.

The business side does not get directly involved in the CAW process. Yet, it is a particularly important element because it determines the strategic objectives of the organization. They underpin the policies that govern the way flight operations and maintenance operations are conducted in relation to business objectives, especially in determining the size and nature of operation and its resourcing. Adequate resourcing

is crucial to safe operation. In this respect, an ID should pay particular attention to the operator's corporate policy and management infrastructure. Beyond the company's business objectives are the external factors, national or global issues that influence and shape the company's strategic business objectives.

6.5 Model architecture

Literature research points to several different techniques that could be used to derive a structure of the ID. These are:

- Fault tree analysis [80, 83, 84, 85, 91, 92].
- Learning from data [80, 83, 84, 85, 91, 92].
- Using case studies [83, 84, 85, 91, 92].
- Other techniques: interviews, surveys, experience, expert opinion [83, 84, 91, 92].

Fault tree analysis (FTA), though could be made very comprehensive, is a speculative technique. It produces too many combinations on long drawn out causal chains and too many redundancies, which may be difficult to handle. Although FTA might be beneficial in a small process, but when relating to a complex process, Luxhoj (2002)[83] recommends that it is best to avoid FTA unless no better information and means is available.

Learning BBN from data involved collecting apparently unconnected random data and then attempting to determine a structure of the network; this is called structure learning in Bayesian techniques, which allows the placement of the links in a neural network. However, a large amount of data must be available at the outset, obtained from observations or by surveying. In this study, this condition could not be satisfied as there was no data at the beginning and surveying of licensed engineers at work whilst waiting for errors to occur was not a practical proposition that could be implemented in a busy airport environment. In any event, it should be acknowledged that the CAW environment already exists as an established process through several decades of evolution of civil aviation. Therefore the idea of learning a structure from data in this application was both irrelevant and redundant.

Eliminating the above mentioned techniques, the study was left with retrospective analysis of case studies associated with error incidents, supplemented with information obtained through interviews. Surveys and questionnaires were eliminated on the basis that individual engineers did not want to divulge internal practices that lead to errors because of fear of recrimination from management and job security. Indirect evidence to support this assumption has been observed.

Analysis of case studies, supplemented by experience and expert opinion gave more accurate information. The study was also supported by UK CAA, Regulator, where expertise was available.

Having considered these alternative approaches, the preliminary structure of the ID was set on the basis of experience and expert opinion. On the question if this method has any academic precedence, Yin (2009)[92] has confirmed that, in soft science, even the use of a single case study to develop a generalized causal chain is a valid technique for generating a structure.

6.6 Design of high-level ID

Following technical logic, and taking a top-down approach, an exploratory design of an ID was produced, which integrated various authorities and functional organizations participating in the CAW process leading to an end product, namely a "revenue earning flight" Figure 6.2. This ID incorporates elements of Reason's socio-technical risk management system[1] as discussed by Rasmussen (1997)[93].

6.7 Dynamic stability of CAW process

CAW is an on-going dynamic process. Errors do occur in the process as a natural phenomenon, but in a well managed system these errors are observed and rectified before they become a hazard to the end product. As long as errors are defended or remained dormant, and the end product is protected this way, the CAW process can be considered as dynamically stable. Where an error has escaped both detection and defences, and has migrated into the flight phase leading to a flight incident, it can be considered that the CAW has become unstable at that occasion. What major factors contribute to the instability of CAW process and risk?

6.8 Major factors that influence risk

Principal factors that influence risk have been represented in the ID, as:

- Compliance with EASA Regulation.
- Performance of Part M AO responsible for CAW of aircraft.
- Performance of Part 145 AO maintenance provider.
- Performance of Part 21 AO that provides post-design services and product support services, i.e. advice on design issues and integrated logistic support issues.
- Performance of individual licensed engineers and managers.
- Performance of corporate business organization that sets corporate policies.
- Effect of global and national level external influences, e.g. global economy, fuel prices, global terrorism and post 9/11 security policies.

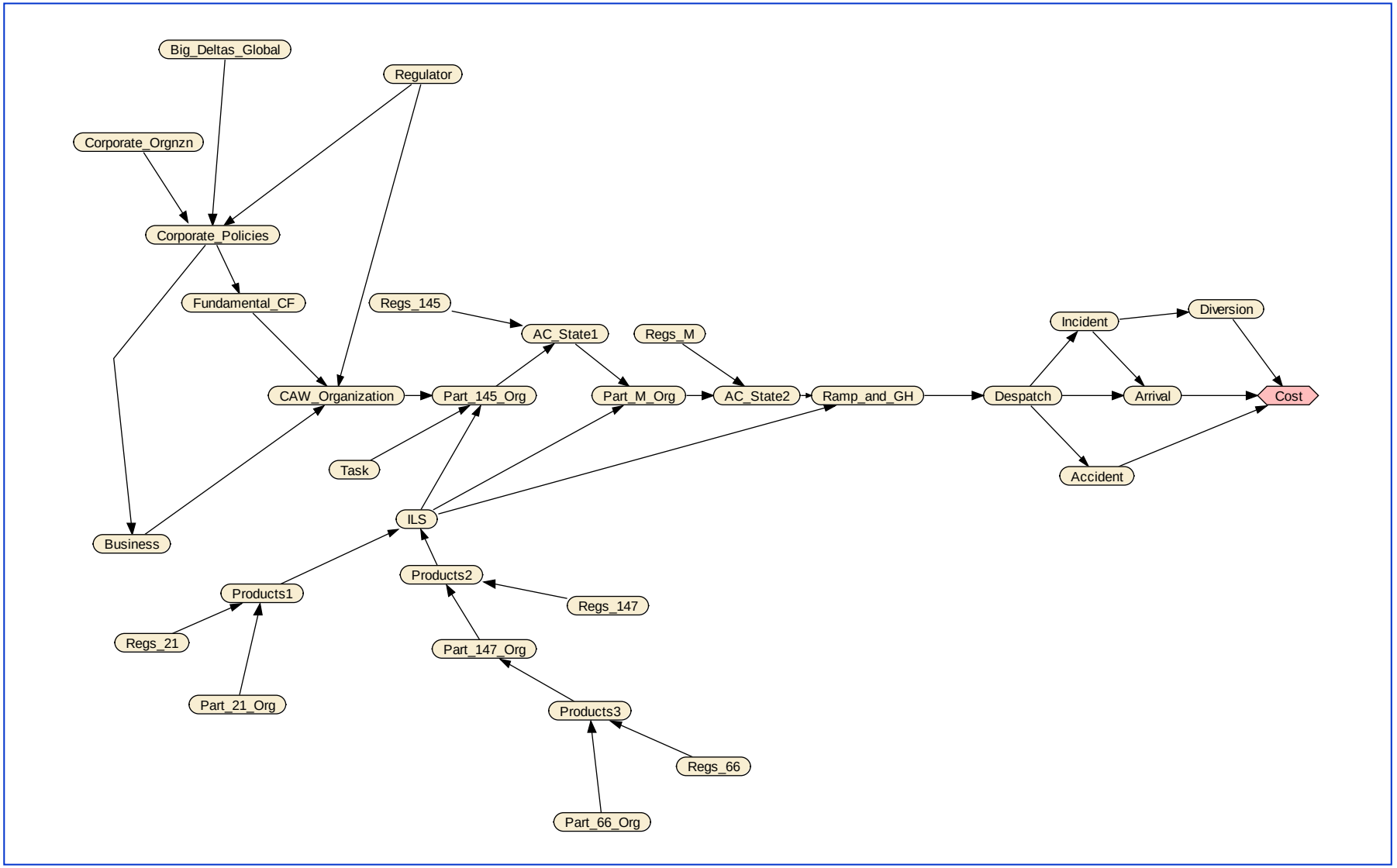


Figure 6.2 - Exploratory design - High level influence diagram for CAW process

Intentionally Blank

- Defences and interventions.

A graphical presentation of the high-level ID encompassing all these major factors is at Figure 6.2; its rationale and composition is described in Appendix 3.

The performance of the individual is very much at the hub of the risk issue. His training and qualification, skill levels and licensing may be controllable. However, many other factors that affect their performance cannot be standardized or controlled; some important ones are their personal traits, physical and psychological make-up, domestic conditions, sense of job security, and tolerable individual stress thresholds, as well as their health and welfare.

According to Regulation, an AOC Holder has the ultimate responsibility for the safety of aircraft that it operates. To ensure that this responsibility could be effectively discharged, the AOC Holder may incorporate within its organization a Part M AO and a Part 145 AO maintenance provider; they may be either an integral part of the AOC Holder organization or if not outsourced. In this case the ID has represented the associated Part M and Part 145 interconnected such a way that they make contributions to the safety of a flight. There should be satisfactory integrated logistic support activities to provide maintenance and CAW process functions, as well as post design services and product support from Part 21 AO.

The defences and interventions system is built into the organization, and into the individuals who work in the organization through their training. A more obvious manifestation of the defence system is the Quality and Safety Management System, and a less obvious but an effective form of defence is the human factors training given to engineers.

Directing the entire operation of the interlinked AOs is the corporate business organization that sets commercial objectives from which management policies for individual specialist departments evolve. The root of all funding decisions, as well as the pace of performance of the operation, is set at the corporate business organization, and so it has a profound influence on risk. Corporate business too would have to respond to national and global influences, but unfortunately, other than containing those external effects corporate business is unable to pass on responsibility for error and risk in their organization to external agencies. That is the current state of nature.

6.9 Role of Part 147 Training Organizations in the model

Part 147 TO has been represented in the ID, because of its training role in generating licensed aircraft engineers. There is a strong view amongst experienced, senior

licensed aircraft engineers and managers that the quality of some newly qualified engineers coming into civil aviation leaves room for improvement. Part of this criticism is rooted in the shift in training methods from the traditional 3-year aircraft apprenticeships where budding engineers learnt their trade in a predominantly practical environment. In contrast current methods are predominantly based on computer based training (CBT) in a class-room with very limited hands-on practical experience on hardware and pressure conditions at the workface.

Inclusion of Part 147 TO in the network would have given the opportunity to identify training related causal factors that contributed to human error.

However, UK CAA Personnel Licensing Department advised this study that once an LAE was recruited the responsibility for bringing him up to the required standard lay with the employer through continuation training. That, together with the fact that the standard for LAE is controlled by the licensing authority, infers that the Part 147 TO could not be faulted retrospectively for human errors made by newly rated LAEs. Oversight of Part 147 AO should pick up any weakness in the candidate selection and training process. Part 147 TO was therefore excluded from the network as an agency that has no direct influence on the airworthiness of an aircraft.

6.10 Cost utility

Rounding off the graphical representation of ID, a utility node was incorporated into the ID to represent the significance of failing to deliver the end product as safe as intended; this knowledge was considered of value to managers who operated, audited or supervised the complex system.

Whilst this ID helped to visualize the relationships between various interest groups and functional organizations, it was only a starting point towards producing a risk assessment model (RAM). To make the ID usable with data, it had to be further decomposed and restructured.

6.11 Decision points

An ID should represent the decision situation at a particular time, i.e. to inform the manager the probability of errors being present at critical points in the CAW process. Release to Service or Handling & Despatch are such nodal points where knowledge of the airworthiness of the aircraft is absolutely crucial. Pre-flight maintenance of the aircraft is usually competed at the point of Release to Service. At Handling & Despatch, an aircraft that has undergone preparation for flight and Released to Service is transferred to flight operations responsibility. Pre-Takeoff check just before

the beginning of the take-off run is another critical point where knowledge of the probability of errors might be beneficial.

Usually the CAW process terminates at Handling & Despatch, unless an aircraft that has left the gate returns to the gate or needed engineering support, say, to rectify a running defect. Therefore, for practical purposes, the effectiveness of the CAW process could be measured as the probability of an error being present at Handling & Despatch.

6.12 Error occurrence, detection

Associated with these decision points are the upstream events of preparation of an aircraft for a flight where errors could occur. At downstream, there may be other events that are the consequences of errors, which might manifest themselves or detected by flight crew after the aircraft was transferred to them. Their responsibility for the aircraft and for the handling of errors and incidents extends to the point where the aircraft was received at the destination gate.

6.13 Defences

The organization contains defensive elements that provide defences against potential errors; the defences themselves may be effective (i.e. error detected) or ineffective (i.e. error missed); these should be represented in the ID.

6.14 Consequences

In order for the ID to represent risk level of an approved organization, it should have the knowledge of the accumulated experience of errors, as well as no errors, for that AO, based on all the aircraft that had gone through the CAW process within that organization. The ID should represent all the accumulated experience of consequences, as well as information on those flights that had been completed without an incidence. It is this information that directly influences the decision if, at any time, the CAW process undertaken by that organization is free of risk or not.

6.15 Depository of cumulative experience and pattern detection

To retain the accumulated experience, the ID must be designed as a depository of information that influences the decision making process, as well as the way they are related. This information should be collected, flight by flight, in a sequential form in order to detect patterns of error arising. Some Bayesian software such as NETICA would utilize the patterns of arising to predict the outcome of an error, i.e. if it would

migrate to the critical points or, if not, be detected and neutralized before it causes a consequence, as explained in "Section 10.2, Experience", of NETICA User Guide[90].

6.16 Mapping

Following on from Section 5.6, Bayesian learning, nodes of the ID represent the events of the CAW process, arcs represent the relationship, i.e. the dependencies, sequence of events and direction. If the objective was to represent the decision making process on the basis of cumulative experience, then it was necessary to map significant events in the CAW process originating at different parts of the organization to the appropriate nodes of the ID.

Events assigned to the nodes of an ID have certain states of nature. States of nature, simply identify if an error is present or not, and if an error is present, then what the causal factor is. This information is embedded in the node. Similarly other nodes can register defences, and where these were missed then the consequences and their states, e.g. severity.

6.17 Data requirement

It has been recognized early on in the study that a model could not be designed in isolation and availability of data must be taken into account. If not the model could not be validated in the CAW environment. The study needed to collect data on errors due to various hazards in CAW processes and organizations, defences employed, if error detected and consequences if errors caused damage. Appendix 4 provides a brief description of hazards. Information on errors and error reporting systems are described in Chapter Three, Section 3.21 and Section 3.22. Appendix 5 explains how this study has analysed consequences.

The decomposition of the high level ID depended upon a greater resolution of activities in different participating approved organizations, and within them what incidences occur and what are the causal chains for these incidences. Again, experience and expert opinion was utilised for the breakdown. But expert opinion needed substantiation using information and data from the field, i.e. from a practical experiment.

6.18 Experiment

In hard science usually an experiment is conducted to obtain data. But in soft science approach, where people are part of the problem as well as ingredients of experiment, simulation does not work well. People behave differently under controlled conditions. Therefore it is more appropriate to use data that could be obtained from relevant

situations where and when people have already behaved naturally. Such data are available in operator's proprietary databases but they are protected because of their confidentiality; this study tried to obtain them and some operators responded well.

It is necessary to state here that injecting faults to a live system and wait and observe an unsuspecting engineer to pick it up, or not pick it up, is not something that could be experimented in busy hangar or ramp environment. It was considered if such a simulation could be tried out in an engineering training school, where safety and time-pressure were not critical issues for conducting the experiment. However, the school environment is far too relaxed and the presence of the researcher/ observer would undermine the spirit of the experiment.

The idea of Questionnaires was abandoned at the outset, because employees are not authorized to disclose sensitive information that the study was trying to collect. Consequently, formal requests had to be made to approved-organizations' Accountable Managers, seeking their participation in the study program.

6.19 Data types

This study followed the view that an organization working under natural conditions was the ideal experiment, and data that was generated under such conditions were the best ones for analysis, provided such data could be captured. Fortunately such data are available in civil aviation, and the study originally targeted 3-different types of error data recorded by approved organizations, namely:

a. Investigation reports from Maintenance Error Management System (MEMS) maintained under UK CAA Civil Aviation Publication CAP 562 Leaflet 11-50, formerly UK CAA Airworthiness Notice 71.

b. Mandatory occurrence Reporting (MOR) system under CAP 382 procedure.

c. Air and ground incidence investigation reports that did not fall under MOR procedures.

These were expected to be supplemented by data from Quality Audit findings, and formal regulatory oversight Findings by the NAA.

At an early stage of the research study, UK CAA denied access to MOR data on grounds of confidentiality, causing the study to rely entirely on data that operators were willing to provide voluntarily.

Selective error incidences undergo detailed investigation (called under MEDA process – MEDA stands for Maintenance Error Decision Aid) that identified causal factors, and

end up with a final management decision on their disposal or corrective actions. These together with minor MEMS data were considered to be a better source because error incidence data were more likely to be available in sufficient quantities from any one controlled group.

Flight incidents due to CAW error are relatively rare occurrences in one controlled group, even though they could be included in MEMS data. One problem with minor errors was that most of these errors are usually classified as at the "bottom of the error iceberg" and considered insignificant by management hierarchy. They could thus be absorbed into the routine activities, put away without investigation, or dealt with as a routine matter. Nevertheless, it was decided to follow up MEMS data.

6.20 Participant operators

Anticipating data requirements for the validation of the model, a number of airlines and MROs were invited to participate in the study programme. Some have accepted and agreed to provide data, but others either turned down the request indirectly, ignored or simply pretended to be helping and gave nothing in return. Company proprietary data are highly sensitive, and safeguards had to be set up to protect company's interests before they could be released. These were done by signing Confidentiality Agreement relating to security and desensitizing of published information. These airlines and organizations acted as the controlled groups.

6.21 Pilot study

Under this collaborative arrangement, a local regional airline (Airline A) provided a sample set of data for a pilot study, namely incidence reports and MEDA investigation reports. These were further analysed, and appropriate causal chains were drawn up.

Appendix 6 identifies the relevant case studies from this pilot study and, Appendix 7, the results of the analysis and respective causal chains.

Results confirm that causal chains arising from an error/incidence in one location of the CAW process could propagate through the whole infrastructure, to higher level of the hierarchical structure of an organization

It was observed that local Investigations usually stopped within a set of boundaries leaving incomplete lines of investigation, open-ended at points where there was transition to resourcing and policy side. Causal chains should cross over to other approved organizations, such as Part 145 AO to Part 21 AO, where root causes for a human-machine interface error originated, but these chains had been discontinued.

In such cases, investigators scope might have been limited by their individual sphere of knowledge, capability and authority. But the most likely reason was that only minimum effort should be spent on investigation that would be sufficient to close the error report; this may be a commercial viewpoint and judgment. However, from a risk assessment viewpoint relating to strategic issues, wider issues, for example, the direction that the causal chain would take outside the frame was relevant to the research objectives.

Both issues, i.e. the limitations of MEDA investigators and the possibility of extending causal chains outside the MEDA investigators operating boundaries, were discussed with the data provider's specialist department (Safety and Quality). The conclusion was that extending the causal chains to their likely root causes was valid, but alternative decisions had to be taken on cost-effectiveness, as well as the way the business was run. The data provider confirmed the validity of causal chain extension applied to researched case studies despite business orientated practical limitations.

This is an important precedence in so far as the research objectives are concerned, relating to fundamental causes that underpin error generation, namely: initial design, production, support planning, training as well as corporate policies and resourcing.

Causal chains so obtained were able to substantiate this limitation almost in all the cases studied. However they did not show a specific pattern, each case offering a causal chain different from others. This is partly because the sample size was small. However, confirming observations made by Yin[92] even with one or few case studies, the sample dataset substantiated the way causal chains are sequenced through organizations, organization level issues, task level issues and individual level issues as per Reasons socio-technical model[1].

6.22 Data requirement – larger scale

Based on this early analysis, a larger scale data requirement for the main model was defined, but keeping flexibility for changes. Since the model would calculate probability of error occurring given a set of conditions, it was necessary to relate this value to usage parameters, e.g. flying hours or flights or sectors flown or landings etc. Furthermore, it followed that all data should come from a controlled group and that boundaries of the controlled group should be defined.

Requested data fell into 3 categories as follows:

- **Boundaries of the controlled group** The first group of data were to be used to define the boundaries of the reference frame of the controlled group.

- **Incident data and incident identification data.** The second group was the main bulk of data. They consisted of incidence and investigation reports in hard copy form or if not as digitised data files.

- **Supporting data**. The final data group was supporting data, to be used for analyzing and interpreting main causal factor data. There was also a need to collect data on flights not affected by CAW errors.

Appendix 9 provides details of the full data requirement as released to participating operators.

6.23 BBN experts' guidelines for model construction

Unlike the demonstration of BBN concept by Luxhoj [84]using error data from one specific structural component, this research study on the CAW process had a much wider scope. According to the outcome of the literature survey, no one else seems to have attempted to design a risk model of this scope. Given that Luxhoj's papers were short of information on methodology, the design and construction aspects of a wide-scope risk model had to be done without a precedent, i.e. from first principles. The path taken is described below.

Given the high level ID (Figure 6.2), the next step was to decompose it so that the practical CAW process could be captured by the network. A missing ingredient was a technique for decomposing the high-level ID to lower level elements.

Given these circumstances and little other guidance to proceed, a suggestion from Clemen (2000)[85] pp 45 was helpful. He suggests that an ID could represent a series of "Fundamental objectives" and "Means Objectives", connected up as a network.

He explains that fundamental objectives are the ones that directly affect the decision. Means objectives are the ones that help to achieve fundamentals. In a network, the upper levels in the hierarchy represent more general influencing factors to achieving fundamental objectives, and the lower levels describe important active elements. Between the means objectives and fundamental objectives, there are intermediate level objectives. Combinations of means objectives could connect up with intermediate levels or higher levels.

This idea was interpreted as equivalent to functional objectives to be achieved to deliver an airworthy aircraft at the end of the CAW process. Fundamental objective is for an approved organization, in this case an aircraft operator, to conduct a safe civil aviation business. Means objectives are the numerous operations undertaken to

generate an airworthy aircraft for the flight. Intermediate objectives could be set as the integrity of aircraft, or processes undertaken by different sub-organization, i.e. Part M and Part 145, as the aircraft is prepared and certified, or the process is supported by these subordinate organizations that provide a service to the principal business entity. Errors occur in hierarchical layers of this structure. Knowledge of the presence or otherwise of errors at different layers, and their causal factors, provides the opportunity to estimate the error contributions from individual elements and groups.

Clemen (2000)[85] further suggests that, although this approach often works, if the problem being analyzed is a complex one and the analysis is done from professional experience, then it may not be necessary to get down to first principles, as long as the analyst has a clear and unambiguous view of the respective fundamental and means objectives.

Given these options, the detailed decomposition of the model was undertaken from an expert's viewpoint, supported by the pilot study done with Airline A. That is, since experience was already available, a heuristic approach was taken to decompose the ID and reconfigure it as a working model. This working model incorporated features of fundamental, intermediate and means objectives. It also included all the design issues hitherto discussed in this chapter as well as the characteristics of Bayesian logic converted to a BBN as discussed in Chapter Five. Where relevant, lessons learnt from literature survey have been taken into account at this point of the design. Figure 6.1 (Flow Diagram to Model Design) was constructed to consolidate the knowledge acquired through this design exercise and to demonstrate the road map that may be of use to future researchers in this domain.

6.24 Rationale for decomposition of the high-level ID

The following paragraphs provide further explanation on the decomposition of the high-level ID and reconfiguration of the model.

During the course of this study, the current CAW process has been discussed with CAA experts, high level managers in industry, safety and quality staffs from approved organizations, trainers and representatives of licensed engineers. There is general consensus that although the current system provides a reasonable standard for safety assurance it left many gaps. There is a general acknowledgement that, often, events that actually happen at the shop floor and management chain on a day to day basis are the critical actions that ultimately decide the achieved safety despite the formality of regulatory compliance. NTSB or UK AAIB detailed investigation reports of CAW error attributed aircraft accidents substantiate this view

Thus, it is absolutely essential that "safe performance of the organization in CAW processes and their management" is represented together with "regulatory compliance" within one model because an unsafe act may well be non-compliance from regulation at the time of its commitment. Meeting compliance and delivering a safe CAW process are concurrent, parallel, activities that lead to the integrity of the end product. These objectives lay at intermediate stages between the fundamental objectives of the business entity and the end product. It follows that at a higher level the model should represent the business and its corporate policies, external factors that influence the business, and departmental policies that integrate the full operation at least to the extent of identifying the CAW interface. This is because the scope of the study is limited to CAW issues and its parent associations only.

The business, contractual and management interfaces are important because it is at the interfaces where the objectives change from financial to engineering (hence safety) or vice versa. Independent business decisions are made upstream of the interface. At downstream, errors may be made if the CAW organization is unable to cope with the business demand, or in reverse, business terms might either impede or deny engineers from getting necessary specialist support promptly, say, when under time pressure.

Causality of the CAW errors may lie in a prior business or corporate policy decision. For example, commercial policies of an organization might directly influence airworthiness decision process through time pressures put upon the individuals who work in the CAW process. In contrast a CEO or his deputies might claim that they never put pressure on employees or that they are not aware of the pressures upon the employees, and that the employees are expected to report undue pressures and stresses[95].

Unfortunately, employees depend upon the organization for their job security or career prospects; thus instead of reporting pressures they are more likely to act under duress, occasionally erring, in favour of the organization when put under a stressful situation. Middle managers tend to use their positions of authority to prevent, block or inhibit the subordinates from making reports. This is the reason why there are confidential reporting systems, such as CHIRP/MEMS, despite managers' public denial of malpractices.

Because of complexities of this nature, the language of communication too changes at the interfaces. Therefore it is imperative, that the outcome of the CAW process, or more importantly the implications of improper CAW process, is reconverted to a language that the businessman understands. A cost utility at the end of the network would satisfy this need.

In general, once corporate policies are set and the CAW organization has been harmonized to meet the business need, then CAW may tick over as a dynamically stable process. Errors might arise in the system and be either defended or resolved through small adjustments to the system. However, any changes to corporate policies might have significant implications to the dynamic stability of the CAW process, and therefore such occurrence should be represented as parameters that influence CAW decisions. Routine review of Maintenance Organization Exposition by the operator and regulator is a case in point that highlights the importance of change management.

Size of the operation and its resource capability is another important consideration. A large complex operation involving a fleet of several hundred aircraft is expected to generate more hazards, and in the first impression a greater risk, than a smaller operation with less than 10-aircraft. However, what is more important is the balance between the size of operation and its resources to meet the challenge. For instance a small operator who is operating the airline on a shoe-string budget might have an operation at a higher risk, than another larger operation that is well manned by qualified people. Although this may be the first impression, in practise, it might be found eventually that such generalization would not remain true. For example, one could argue that the ratio, fleet size to engineering staff complement is a better indication of its resource capability to deliver a safe continuing airworthiness process. Rating of the demanded pace of work is another important factor. The network should represent these influencing factors.

Apart from the defences built into the CAW processes, the Quality Management System is the main organizational defence against shortfalls in CAW organization and practices. If a QMS functions efficiently, it could pre-empt any shortfalls or weaknesses in the organizational compliance with regulation. Therefore it is bound to be a strong influencing factor on CAW of the end product.

A summary of the current oversight process was given in Chapter Two and Chapter Three. This process is principally based on an audit of the organization to ensure that it complies with the applicable and relevant safety regulation, and if it has sufficient strength and capability to sustain the declared objectives in its formal Exposition.

6.25 Model

The initial idea for decomposing the high-level ID was tested by examining three known models for risk management to see if there is a commonality of features between them. However these models had neither been purpose designed as risk assessment models nor were using BBN techniques as this study was pursuing. They

were common sense evolution of management models based on practical experience. The models were:

- A model produced by Marsh[17]to capture the current oversight process as practised by UK CAA. It uses expert judgement based on evidence.

- MCDA/AHP type oversight process currently practised by the CAA of the Netherlands[62].

- Aircraft Structural Integrity policy for the Royal Air Force[96]. The policy effectively sets out a management model to minimize the risk attributed to potential structural failures of military aircraft.

Features of the three models were decomposed, compared and results are reorganized and tabulated in Appendix 10, under assumed high-level groupings. Although the comparison is not perfect, a pattern emerges from that, sufficient to give confidence that the idea for decomposition and regrouping is fairly correct. That may be considered sufficient for setting a heuristic layout.

As an outcome of this comparison, it became clear that the process of minimizing safety risk needed a holistic approach, all elements of the organization working together as an integrated system. For example, the idea of the top level managers looking for workers to do all the sacrifices is taken out of this equation, by putting the managers in the equation; likewise, while QMS may have an audit role, they are just as well important as defences against error or even themselves as causal factors for some errors. The concept assumes that everyone in the system is susceptible to make errors as well as capable of acting as defences. Guided by this holistic approach, it was possible to synthesize the information and to observe patterns between the 3-systems chosen in this occasion.

- Size of an operation should be compatible with its capability.

- Corporate policies should be compatible with flight safety objectives, particularly on strategic planning, resourcing, and promotion of a safety culture.

- Regulations should be earnestly complied with and not treated as just a process needing a “tick in the box”.

- Performance of the CAW process should be monitored such a way that error generation, as well as good performance, is measured and acted upon.

- Safety and quality audit programme should be effective and not just a safety-cover to the CEO.

- There should be a dynamic and effective change management system that could respond to changing strategic influencing factors (Deltas) that has an impact on flight safety.

Appendix 8, points to the strengths, similarities and relative gaps of the 3-system, and offers a possible way forward for combining these indicators in a new proposal that could provide a more comprehensive risk assessment system. Assessing risk by accounting for errors in these 6-functional areas was considered to be the intermediate level objectives for the model as mentioned by Clemen (2000)[85]. In reverse, if errors are eliminated from each of these 6-areas, then the risk level of the entire operation could be reduced.

Using the foregoing analysis, the high level ID was redrawn as a block diagram with a number of functional subsystems, each identifying with the group that individually influences the airworthiness process and decision taking (Figure 6.3).

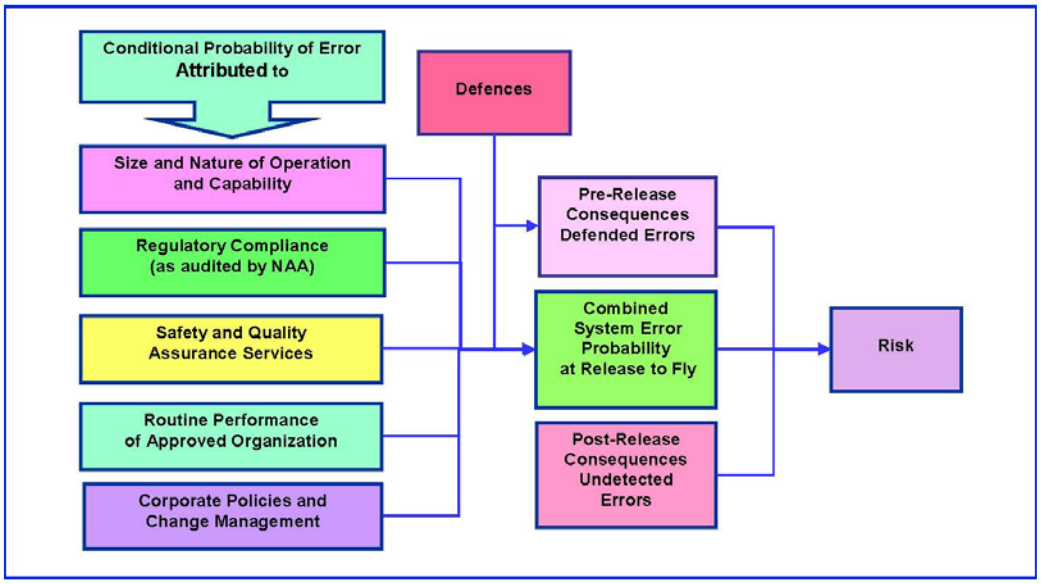


Figure 6.3 – Block diagram of the model

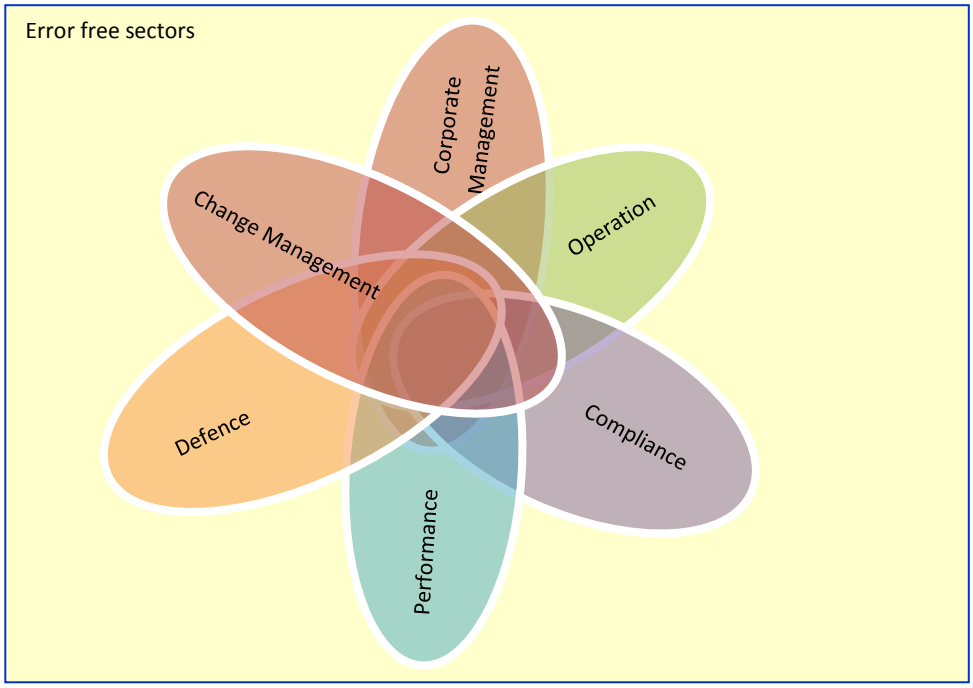
The subsystems are:

- Size and capability of operation

- Compliance with regulation.
- Routine performance by AO in its tasks.
- Performance in safety and quality audits.
- Corporate policies and change management.
- Consequences.

Human errors occur within these sub-systems, singly or collectively, which could cause system errors. The probability of a system error occurring, when combined with the severity of consequence would yield a risk value. The configuration acknowledges that error generation within each subsystem occurs independently from what happens in other subsystems. However, when it concerns the safety of the end products from the organization, then these separate subsystems has interdependency through the end product.

The joint probability of a system error occurring could be visualized in Figure 6.4 as a Venn-Diagram. The box represents all operations of which the majority are error free. Each (free-floating) oval shaped subset represents probability distribution of different types of error attributed to any one subsystem. Their intersections represent system error probability attributed to two or more subsystems and any error lining up. Note that shapes, sizes and intersections are not to scale. This is one snapshot of a dynamic system.



Figures 6.4 – Visualization of system error probability

Quantification of risk can be achieved through a statistical probability of system error and estimated cost of consequence. The main part of the model will address the probability of system error. An appropriately designed BBN to represent the system should be capable of combining the probability of error in each sub-system and returning a joint conditional probability of system error.

6.26 Taxonomy

Implicit with the design and construction of the model, facilities should be provided to upload data. In order to proceed with the construction of the model, prior information on taxonomy for data is required. Therefore taxonomy issues are discussed here.

6.26.1 MEDA taxonomy

This study primarily followed MEDA taxonomy, complemented by some features from the HFACS (ME) taxonomy. This is because MEDA is the most widely used taxonomy by UK and international airlines, and therefore there was greater likelihood to find error data from participating approved organizations.

MEDA is used in error investigation, specifically in Part M and Part 145 organizations. Causal factors for some errors that occur in Part M or Part 145 AOs might lay in other organizations, for example design shortfalls or errors in aircraft maintenance manuals for which Part 21 organizations are responsible. MEDA taxonomy has made provision to identify such events, though it is understood that the extent of investigation undertaken is rather limited.

6.26.2 Supplementing MEDA and HFACS (ME) taxonomy

In generating taxonomy for this model, MEDA and HFACS (ME) identified parameters were supplemented on the basis of researcher's experience and advice received from subject matter experts in industry and Regulator. For instance, "contractual interfaces" where errors occur is one such addition.

Field research during this study has revealed that unless an error incident has a serious safety implication, little follow up action is taken by airlines to pursue the matter to root causes and to prevent recurrence of such errors. Some evidence gathered during this study substantiated this view. It has been pointed out to the researcher that often the way the commercial side of the operator's business is managed, follow up investigations of most error incidences at Part 21 organization are considered as non cost-effective to either the operator or the Part 21 organization.

6.26.3 Contractual interfaces

In contrast, from a safety viewpoint, the study observed that the contractual interface between the operator and the Part 21 organization is generally a weak area where conflict between safety and profit exists. Inhibited two way information flow, reluctance to investigate defects, investigations shrouded by commercial or legal sensitivities have been identified as the main factors that lead to management decisions in favour of commercial interests.

A well documented example of this type of conflict is the principal parties' failure to find a lasting solution to the long known problem with Concorde aircraft's main undercarriage wheel tyres when damaged by runway debris. In the final similar incident involving an Air France Concorde, the aircraft was destroyed in a tragic accident that cost 109 lives and ended the Concorde program[9]. On the question of blame, according to the judgment given by a Court of Law in France, it is reasonable to infer that there have been high level management decision errors made between the Operator and the Design Authority; they failed to follow up adequately previous, somewhat low profile incidents, and so failed to generate a lasting design solution to the original design shortfall.

6.26.4 Corporate policy

Since MEDA was initially intended as a tool to help investigation of error at human-machine interface, it has a poor resolution relating to root causes that may lie in the upper levels of an organizations hierarchy (i.e. corporate policy or change management). Data to populate those nodes in the corporate policy and change management networks might not be found from MEDA records. Similarly, MEDA is not relevant to regulators oversight inspections, and therefore error data relating to compliance would have to be extracted from regulators in house records, subject to conditions.

In the more recent time, commenting upon the inadequacy of MEDA taxonomy, UK CAA paper 2007/04[53] has introduced three categories of maintenance error for the purpose of analyzing some 3,000 Mandatory Occurrence Reports (MOR) accumulated over a period of 10-years. This too supported the view on MEDA's limitations.

6.26.5 EASA regulation

The adequacy of MEDA taxonomy was reviewed with UK CAA to determine if it met the models objectives, especially with respect to regulatory compliance issues. UK CAA was of the opinion that any model that could be used to assess risk under RBO concept ought to have a relationship with specific EASA regulation. This is because

the existing system of legal liability of an operator, i.e. to ensure that the organization and its mode of operation does not constitute a risk to flight safety, could be exercised by identifying the specific EASA regulation that the operator might have failed to comply with.

This argument from CAA's was accepted as a very important contribution to the objectivity of the model from the Regulator's perspective. Moreover, the same argument could be taken forward to assist the operator. For example, if the model is used as a part of the organizations SMS, then it could also be used for self-regulation with respect to compliance requirement. The organization would then have a management tool in hand, by which it could review its level of compliance against the regulation.

Accordingly, EASA Regulation 1702/2003 Part 21[97], and EASA Regulation 2042/2003 Part M and Part 145[98] were used as guides for decomposing the compliance subsystem, and parts of the routine performance subsystem for Part M and Part 145 organizations. Compliance subsystem would capture errors during oversight audits and inspections by Regulator in the form of Level 1 and Level 2 Findings; this subsystem is reserved for this purpose but its data would be used in conjunction with data from other subsystems to assess the overall risk. Any errors in compliance discovered by the operator as a result of incidents would be captured by the routine performance subsystem.

6.26.6 Consequences and cost

Nodes on the Consequence net are not entirely error data, but also outcomes of presence of error and impact on the operation and cost when recovering from the relevant upstream error or incidence, which missed timely detection. Any error detected before an aircraft was declared airworthy for flight operation could be treated as "No Consequence" on the basis that the cost of recovery from the error is part of the routine cost of maintenance. That's the way it is done at present in most organizations. Obviously if a greater accountability of error is required such costs could be included at the appropriate node, as a modification to this network.

Consequence and cost data are included here because the product of error probability and consequence should yield the level of risk. The scale for the risk has yet to be established depending on the results the model would generate.

Detailed decomposition of the subsystems according to the taxonomy adopted is tabulated in Appendix 10.

6.27 Overview of model construction with BBN software

The model was constructed in stages, i.e. subsystem by subsystem, each subsystem individually tested. Once it was ascertained that each subsystem worked well independently, then they were integrated together to form the complete network.

The networks were constructed using commercially available NETICA software that has been purpose designed for BBN work, and marketed by Norsys Software Corporation of Canada. Alternative software packages are available in the market and all of them have various advantages and disadvantages. For examples, at one extreme, programs with reputed names are extremely expensive, whereas at the other extreme those free-to-download software available from internet have no back up support and their integrity is unknown. The medium priced packages with commercially available back up support, all have gaps in technical features. NETICA was selected mainly on the combination of affordability and availability of professional level support. It can produce neat networks when the model is extremely complex, as in this case with minimal crisscrossing of links. There is no facility to use colors to discriminate subsystem nodes in a complex network like this; this is a program shortfall.

The construction process starts with the definition of the taxonomy for the nodes, their states of nature, and the conceived architecture, i.e. the direction and relationships between nodes, and their hierarchy; these were discussed in the previous sections. The next task is to transform the concept into a tangible model and transfer the knowledge about nodes and states of nature on to the model. Only then would the model be able to undertake computations using data that would be input at alter stage.

NETICA program is the "tool" that helps to construct the model and uptake knowledge, done concurrently. NETICA provides the graphical representation of the belief network, as well as the mathematical relationships between nodes, and within the nodes. Relationship information is embedded with the node and normally remains hidden from view. But the software enables the relationships to be examined as hidden files, as and when required. Most importantly, the algorithm based on Bayes' Theorem for conditional probabilities, used for computation of error probabilities at any point in the network, is built into the program. The algorithm is Norsys' proprietary information that is not available to public.

The basic steps of construction are:

- Defining the nodes of the model, as these are the main "bricks" of the construction.

- Entering pre defined states of nature.
- Placing the nodes in the correct relationship or hierarchical order.
- Connecting them with links.

All the necessary instructions for the construction can be found in NETICA User's Guide (2003)[90] or in NETICA Help Files located in the program software. Like any other software program, the user must familiarize with the program before using it, or preferably attend a structured NETICA course.

6.28 Model construction

A necessary first step of the construction was the laying out of the high level subsystems described in Section 6.25 as a network. This has been done at Figure 6.5, following which the construction of subsystems began.

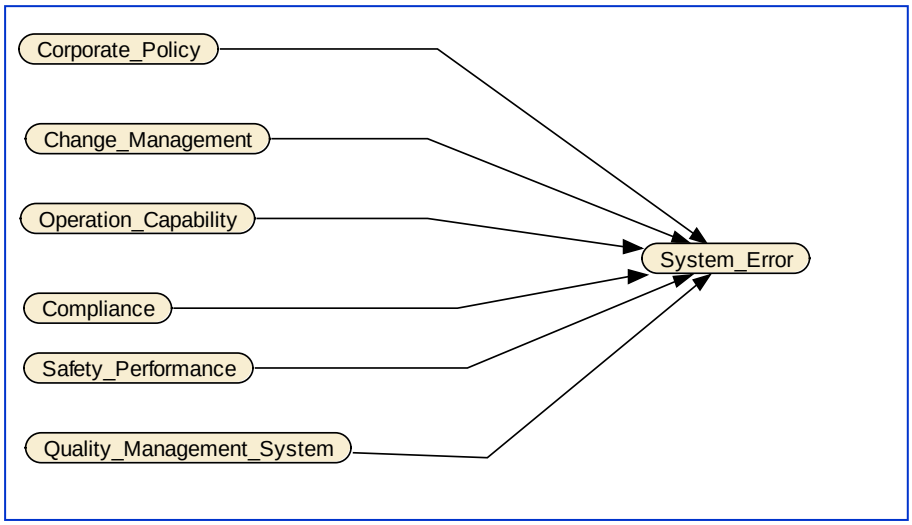


Figure 6.5 - The aggregate - First level of decomposition

The following sections highlight some salient factors taken into account during the design of each subsystem of the model and refer to the final evolved architecture after each design has gone through an iterative design and review process. Early designs, which are now redundant, have been omitted in order to avoid clutter and improve clarity of this document. However some of the important Regulator inputs that arose during the iterative process are discussed in Section 6.30. These discussions centered on the first detailed model (Figure 6.16, now obsolete and enclosed for reference only). Resulting amendments have been incorporated into the final design, which is outlined below.

6.28.1 Size and Nature of Operation and Capability

Size of the Operation and its Capability is in essence the main infrastructure of the aircraft operator. Some of the information gleaned from Marsh[17] on ROWI model has been used to decompose this subsystem. See Section 4.4 for ROWI Model details. Graphical representation of the subsystem is at Figure 6.6.

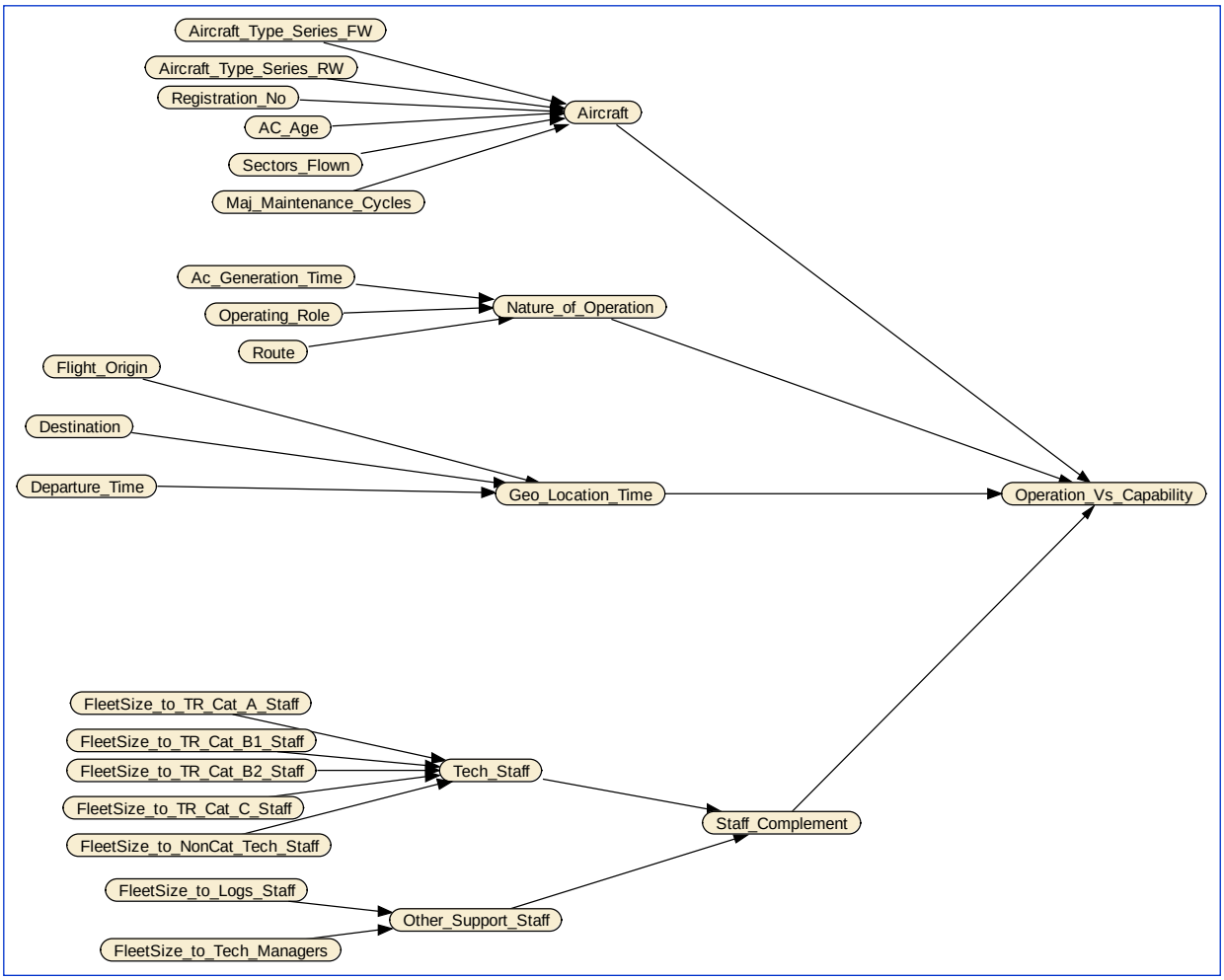


Figure 6.6 – Size of the Operation versus Capability

6.28.2 Regulatory Compliance

The background to the decomposition of the "Compliance" sub-system was explained earlier in Section 6.26.5. Graphical representation is at Figure 6.7 for Part M and Part 145 AO, and Figure 6.8 for Part 21 generic OA.

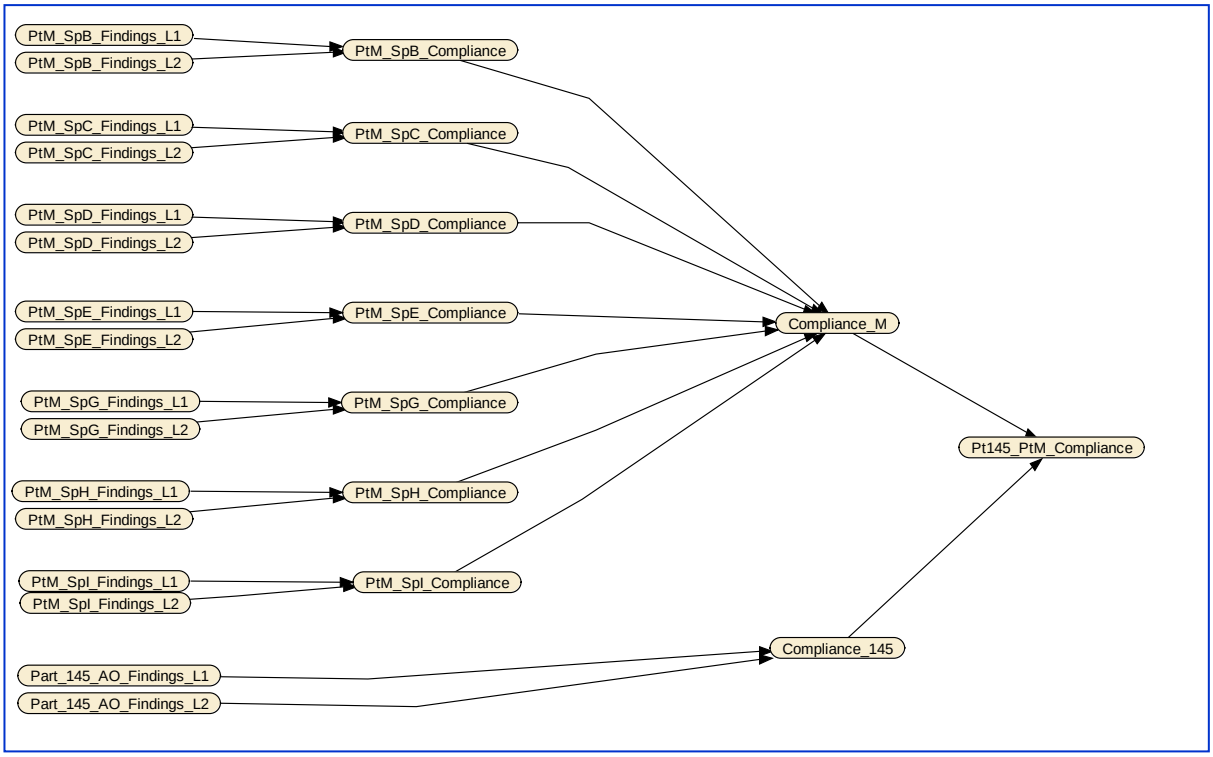


Figure 6.7 – Pt M and Part 145 Regulatory Compliance

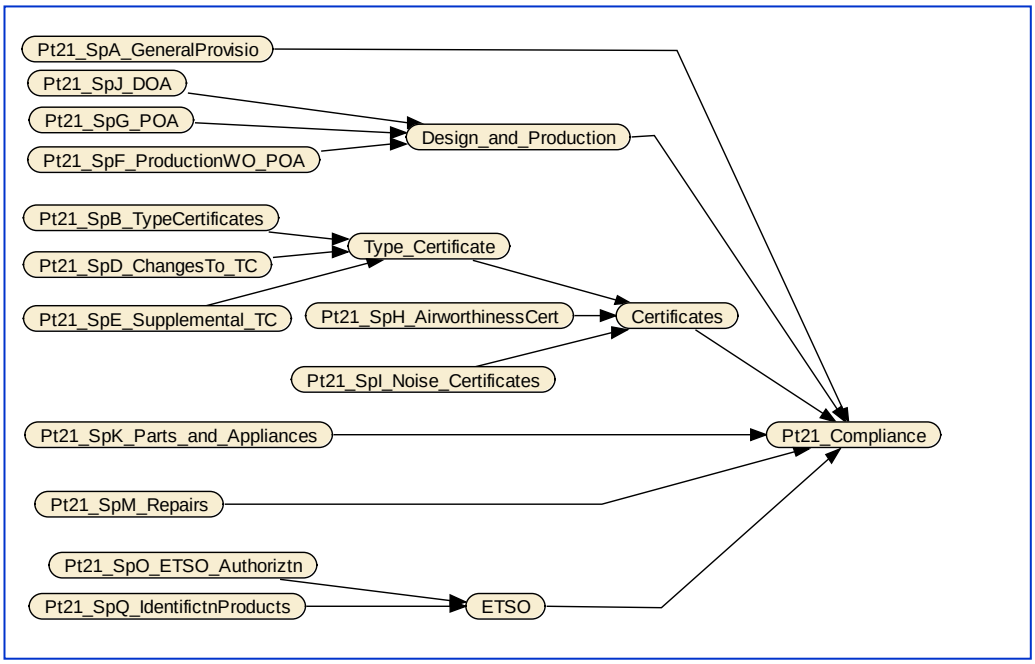


Figure 6.8 –Part 21 generic OA Regulatory Compliance

6.28.3 Routine Performance

The “Routine Performance” sub-system has a complex picture as it demonstrates the synergy between Part M, Part 145, and Part 21 AOs, see Figure 6.9.

The original intention was to include Part 66 licensing requirements and influencing factors associated with a Part 147 Training organization, because of their influence on the quality of Licensed Aircraft Engineers employed by operators. This idea was dropped at this stage of development; the rationale for its deletion was explained in Section 6.9.

Key features included in this subsystem are as follows. Part M and Part 145 organizations are independent in discharging their respective responsibilities. Part 145 AO is the maintenance provider whereas the Part M AO is responsible for ensuring that CAW is assured through the CAW process. This does not absolve Part 145 AO from following regulatory compliance and industry best practices to ensure CAW; they are responsible for meeting that objective unlike some MROs tend to believe. Part M AO specifies the task needs to be done on the aircraft, and formally transfers the responsibility to perform the tasks safely according to EASA regulations and industry best practices.

The legal responsibilities for the tasks and interactive support are defined in the interfacing contract between Part M and Part 145 AOs. Part 21 PDS and Product Support are usually obtained by Part M AO, for which they would have another interfacing contract between Part M and Part 21 AOs. Part 145 AO, if they need Part 21 support, would call it up via Part M AO, unless there is prior contractual agreement for direct contact between Part 21 AO and long-established Part 145 AO.

Part M AO performance is measured against tasks organizational issues defined by EASA regulations and decision nodes that sum up the outcome of upstream events; Part 145 AO performance is measured against regulation as well as key elements of integrated logistic support with respect to organizational issues. It is also measured against capability and other personal traits of the individuals who either perform the work or manage them, and various factors that represent personal and task related factors at the work face.

Part 21 OA performance is linked to the overall performance sub-system, because causal factors for error may well lie in the Part 21 OA. For example an error in the aircraft maintenance manual that could lead to a human error at workface could well be an error caused by poor integrated logistic support planning and management at the Part 21 OA. The decomposition allows errors to be attributed to the most appropriate source, and moreover encourages the investigator of an incident or error

to pursue the investigation to the root cause, unless of course it was blocked or over-ruled by management. In this latter case, the management should account for the blockage.

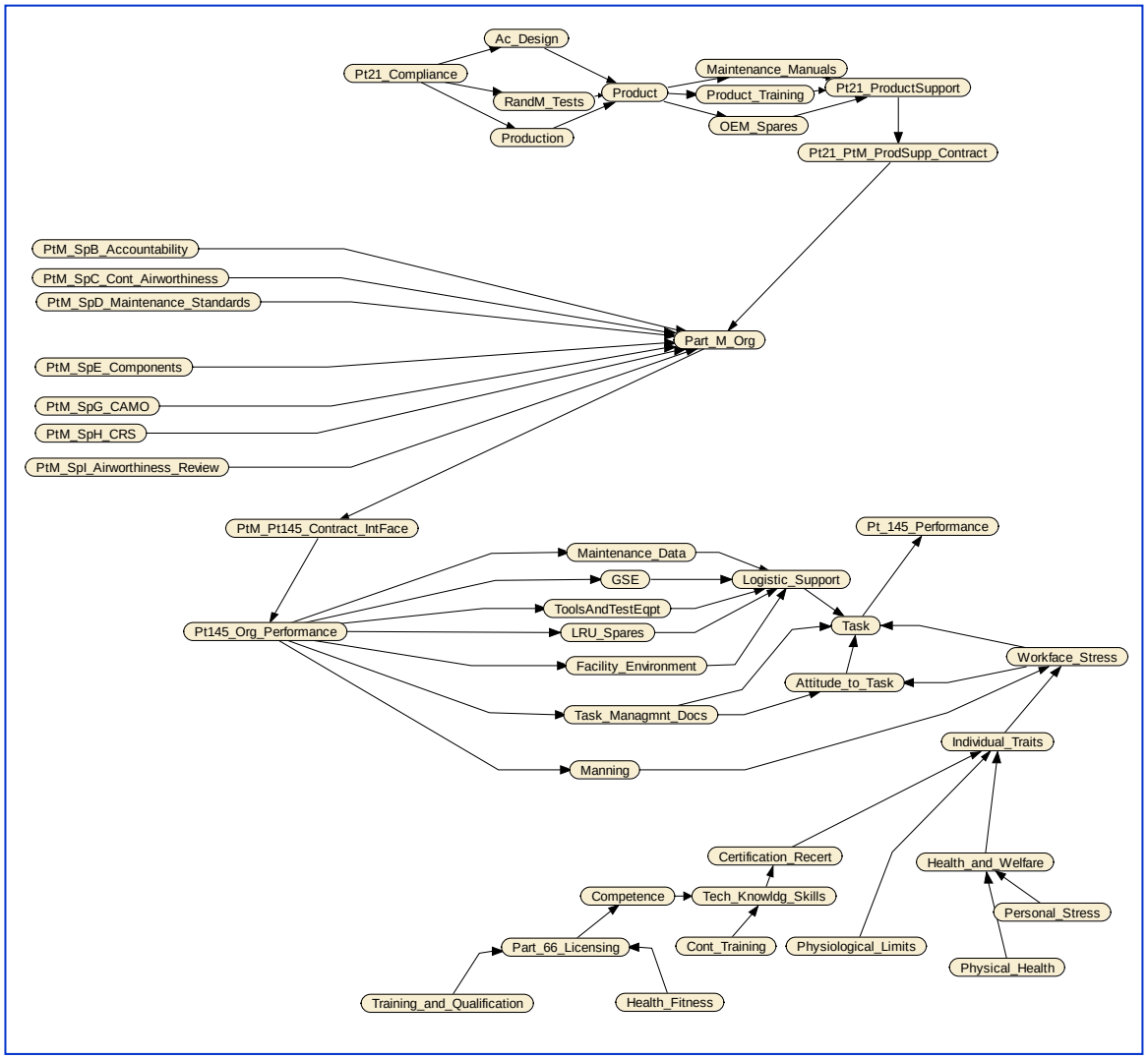


Figure 6.9 – Subsystem Operational Performance

6.28.4 QMS Defence

Decomposition of the Quality Management subsystem was based on the broad requirements outlined in EASA Regulation 2042/2003 Accepted Mean of Compliance MA 712, Figure 6.10. To enable MA Subpart G organization to ensure that CAW of aircraft remain in compliance with Part M requirements there should be a quality management system. It should address CAW Quality Policy, Quality Plan, QA Procedure, QA Remedial Action Procedure and Training and Qualification Standards for Audit Personnel. These objectives for meeting these requirements should be

defined, documented and resourced under the QMS organization, as well as implemented through the QMS infrastructure and program. The detailed decomposition was based on EASA Regulation Part M – MA 712 and Accepted Means of Compliance, supplemented by subject matter expert advice.

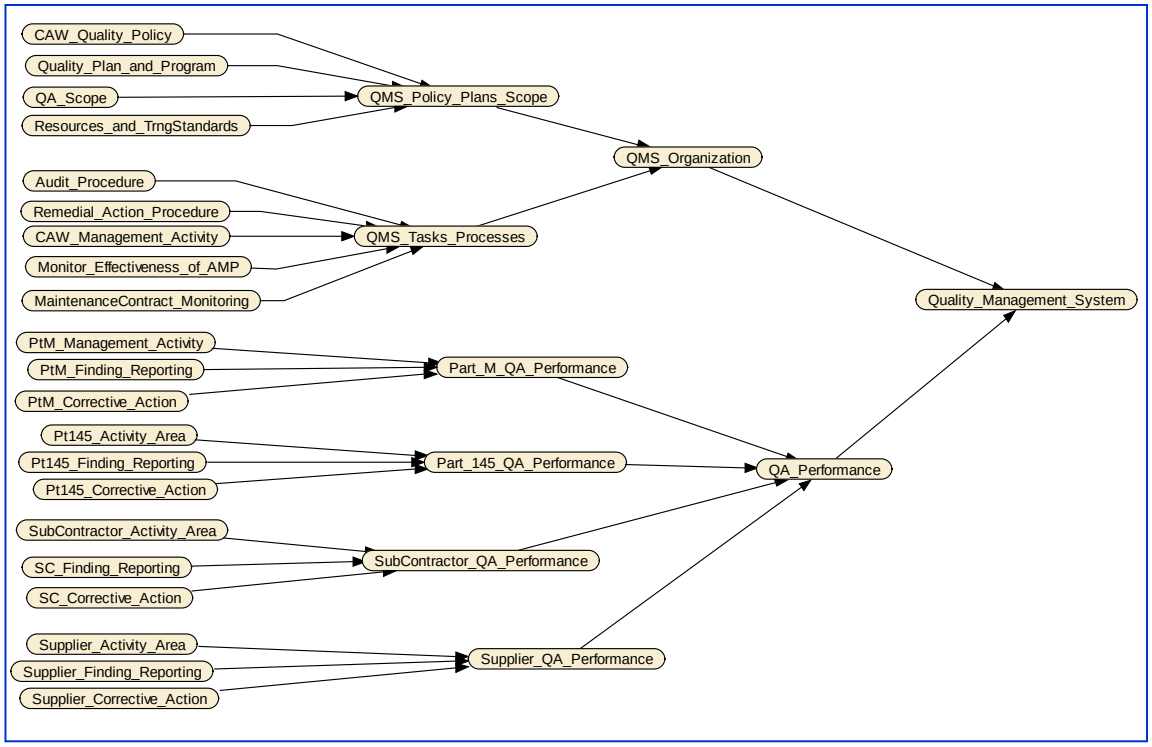


Figure 6.10 – Subsystem Safety and Quality

6.28.5 Corporate Management and Change Management

Corporate Policy subsystem, which includes Change Management extension, incorporates the CEO/AM's unique position as the Chief Executive and the interpreter of the corporate board's strategic policies. The decomposition follows the traditional hierarchical structure of top level management (Figure 2.3). CEO/AM has to take into account external factors that would influence his decision making role and the decisions. Global factors, central and local government policies and objectives, trade unions have been identified here; it is not an exhaustive list, and there could be others.

At the output end, errors might occur in corporate and policy issues that affect CAW processes, but usually they might be dressed as errors of judgment. Origin of errors in specialist departmental policies at high level may be rooted in corporate policies, so they might conflict with safety requirements, with the way CAW process is conducted. Change Management is an extension of corporate policy subsystem. This subset

represents an organization's alertness to foresee upcoming changes or evolution of strategic objectives, to consider the implications and then plan and manage the way the operation ought to respond. Business management, operations, engineering and technology and human resources issues, as well as changes to the existing Expositions have been identified as factors that have significant influences on risk. Errors in identifying changes and in timely responses could cause downstream problems. The network will show how top level decisions could affect safety at lower levels.

At higher levels of the operator's organization, errors are most likely to be called "Errors of Judgment" in order to mitigate their impact, because top level managers tend to protect themselves and the corporation against possible liabilities arising from "management errors". Therefore, in practice, operators might not allow this part of the network to be implemented in their organizations; this is a practical reality. However in an SMS they could consider adopting this principle for their own benefit and long term welfare of the organization. The graphical representation is at Figure 6.11.

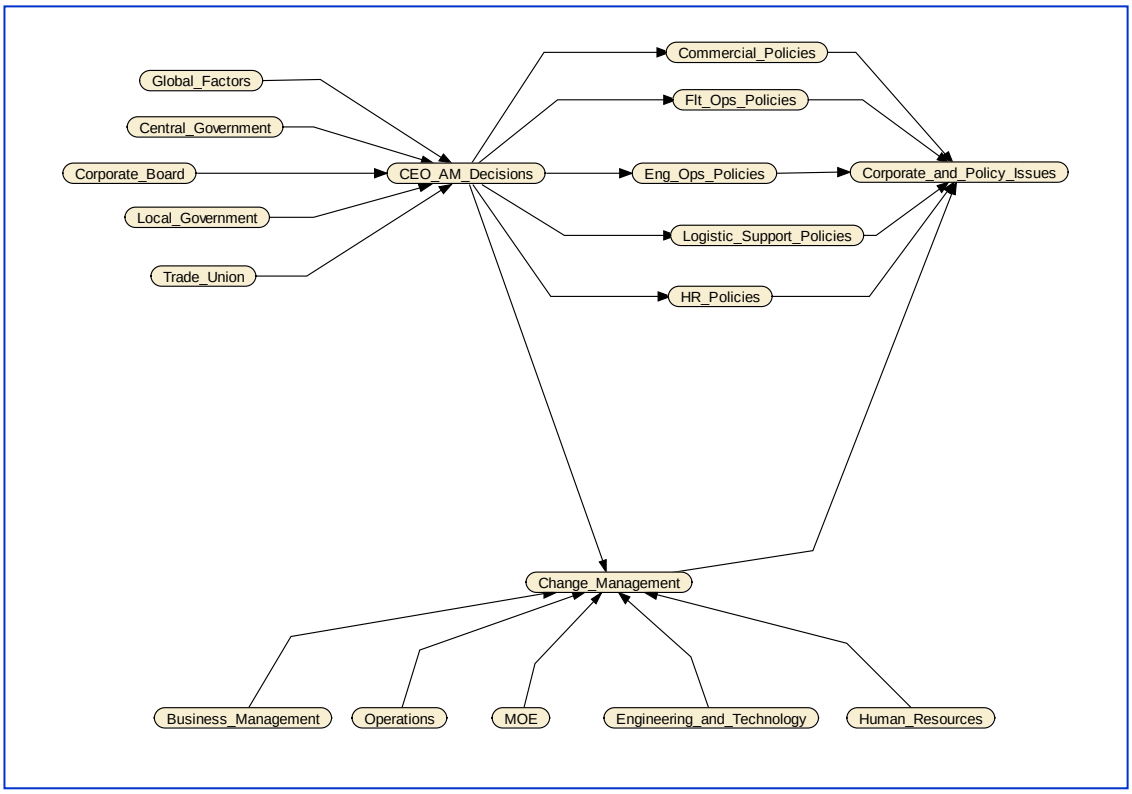


Figure 6.11 – Subsystem Corporate Policy and Change management

6.28.6 Consequences

The “Consequences” subsystem, Figure 6.12, starts at “CAW Management” node which combines/ coordinates outputs from Pt M and Pt 145 organizations. If CAW process is satisfactory it is assumed that the process and aircraft are error-free, moving them on to next progressive stages of “Release to Service”. Note that this document and Netica model uses the terminology “Release to Fly” to describe the same event, which is a critical milestone in the CAW process that places an aircraft fully serviceable and airworthy for the intended purpose. It is done through a process of checks and cross checks of aircraft documentation after having ensured that all engineering maintenance activities have been correctly completed and certified by authorised personnel.

At Handling & Despatch, flight line staff of the maintenance organization share responsibilities with staff of flight operations, until the aircraft is pushed back and aircraft captain takes over the full responsibility for the safety of his aircraft, but within the limits of his terms of reference. Handling & Despatch is a transition point, the last stage of the CAW process. If errors are present and detected, it is assumed that they will be defended by the routine process of stage checking and cross-checking up to this point. It is expected that any errors would be detected by defences, but it is also possible that some errors might escape detection and would get transferred to the next stage of the decision process. It is also possible that new errors get introduced at this stage due to human activity, like leaving a cleaning rag in an air intake or forgetting to fasten an access panel to a ground power cable plug point. Although the CAW process usually terminates at Handling & Despatch node, if there are running repairs to attend to after push back, then CAW process may be extended.

Once an aircraft has left the gate, safety of aircraft is in the hands of Flight Operations with responsibilities shared with ATC and Airfield management. Defence at Pre-Takeoff is done by flight crew, for example, when errors might show up as cockpit indications or anomalies in handling or in aircraft systems performance.

Errors if detected at any stage would lead to a consequence such as delay in meeting the flight schedule, or cancellation of the flight together with associated primary and consequential costs, e.g. hotel costs or alternative transport for passengers. Assuming that an aircraft has left the gate with an undiscovered CAW process error, it might be detected by flight crew if it affects the normal operation and handling of the aircraft.

In the event, if a dormant error escapes detection at Pre-Takeoff , it could continue to remain dormant throughout the flight or manifest itself as an incident before the end

of the flight. An incident would generate a consequential cost. The Combined Cost node pulls together all the consequential costs.

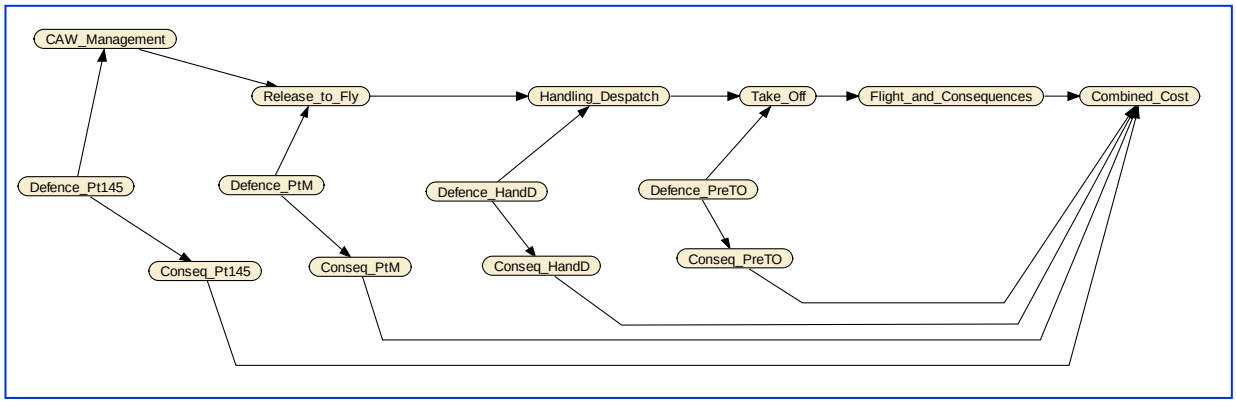


Figure 6.12 – Consequences

6.29 Integration

The form of the model when all the subsystems are integrated is at Figure 6.17. Prior to their integration each subsystem was separately tested with simulated data to ensure that it would compile properly and that it would produce a meaningful result. Proof of compilation was particularly important because it confirms that the logic incorporated into the model architecture was correct. Configurations of individual subsystems have been reviewed by CAA experts as part of the established research process. This has lead to more detailed decomposition of Compliance subsystem, providing a greater resolution of causal factors required for regulatory purposes.

Integration proceeded on the assumption that CAW process ends at Handling & Dispatch; so, the probability of error in CAW process is calculated at this point. For this purpose, error probabilities generated at each of the subsystems have been taken into account as connected by arcs from Size of Operation and Capability, Compliance, Routine Performance and Quality Management System. Outputs from Corporate Policies are input through Compliance subsystem, Pt M performance and Pt 145 performance. Input from QMS takes into account outputs from CEO and Change Management; this is because of QMS', special relationship with CEO for Quality and Safety issues of the operation, as well as Change Management's important role in keeping QMS updated on potential implications of policy changes on the quality of organizations performance.

A sequential connection has been adopted to be compatible with the hierarchy demonstrated in the high-level ID. Also a simple decision flow process with series and parallel connections has been followed. This level of connection can be described as a

first order interaction between subsystems and various other constituent elements within each subsystem. In practice, in a complex organization cross fertilisation of influencing factors do take place between subsystems. These second and higher order influences are not represented in this network for several reasons:

- It is not graphically practical to do so in here without cluttering up the graph and confusing the reader.

- This DAG is not a decision tree but an influence diagram and there is no need to represent all second or third order factors.

- The ID is not exactly matching the flow process of activities but following the flow of influencing factors that contribute to the decision, which is, if there is a risk due to CAW error.

- It is necessary to limit the number of potential combinations that could be formed by the whole range of different nodes and states of nature; if not the capability of the computer will be the limitation.

Therefore a reasonable position to adopt is to accept the argument that cross-fertilisation does take place in real life and whatever the state of nature achieved at each event is in fact its result.

It should be noted that knowledge of existing oversight inspection processes has been incorporated in to this model as a springboard. It is an advantage because it provides confidence in the proposed configuration. Moreover, experts who gained their experience in a traditional risk assessment environment would find that the transition to a new method is easy, and the configuration follows what they were familiar with. Thus change management is encouraged and facilitated. The capability provided by this model to convert an organization's human errors to a risk as a statistical probability should be a strong attraction to safety managers in any industry.

Finally, it should be reiterated that to determine the effects of flight incidents due solely to CAW error, the model should assume that no errors are contributed by flight operations, air traffic control and airfield control. This is a reasonable assumption, because in real life, post accident investigation would reveal and apportion contributory elements to each relevant service if it is involved, and CAW process would take its fair share. For the purpose of model construction, it was assumed that all other services were perfect and made no contribution to safety risk, except where cross inputs were taken account at the interfaces.

6.30 Integrity checks on the model and industry expert inputs

As briefly mentioned in Section 6.28, integrity checks were done on an earlier version of the ID (Figure 6.16) to confirm if it correctly represented the CAW flow process, as far as practicable, that potential sources of error have been comprehensively covered, and that the model reflects current industry practices. This task was assisted by UK CAA SRG Airworthiness Standards and Procedures (ASP) Department. The following Sections record the action taken in addressing the key issues raised by UK CAA.

6.30.1 Mapping EASA regulation

A significant step change resulting from UK CAA advice was that the number of nodes increased from the 107 nodes initially started with to 176 nodes. The original layout essentially followed the simpler MEDA taxonomy. The layout that has evolved largely follows EASA Regulation, as a guide to decomposing the Regulatory Compliance subsystem. This is the line that UK CAA had recommended, because if the model had to be credible for legal purposes, then it should shadow the Regulation that both UK CAA inspectors and operators recognize.

6.30.2 Level of resolution of causal factors

Another factor that inflated the size of the data set is the level of resolution required with respect to causal factors, which in turn provides clarity when prioritizing investment to reduce risk. There was a decision to be made at one stage, if to reduce the parameters by descoping the model.

UK CAA's views, as expressed at the 6-monthly progress review meetings, were that the model should not be de-scoped in order to ensure that it provides a fine resolution, to link risk to causal factors. This advice was consistent with other known advocacies calling for a greater resolution of causal factors, i.e. UK CAA Paper 2007/04[53], current work in the revision of MEDA tool, CHIRP/MEMS reports and UK Flight Safety Committee, Maintenance Sub Committee all that support better resolution.

Given the concept adopted and a required degree of resolution, it is inevitable that a larger starting data set must be available to make the model work and to derive a sensible result from the model. However, those who oppose this method of risk assessment might suggest that this demand for a large starting set of data would make the model impractical.

In rebutting the opposition argument, it should be stated that the model does not require factual information all the time. Input data could be estimated using best guess, to be refined later as more and more data comes in. The technique adopted for validation of the model will be discussed in Chapter Eight. Moreover, once sensitivity analysis has been carried out on the model, it might be possible to derive a smaller set of KPI that could be monitored by the Authority. Even so, there ought to be caution until trends are established. This is because conditions could change in time, which would shift the sensitivity from one parameter to another. If not careful, one could end up with monitoring the wrong KPI, when the actual damage is in fact occurring elsewhere.

Other data handling issues raised by UK CAA Regulator during the testing stage are discussed below.

6.30.3 Proactive and reactive errors

Proactive errors are those detected by engineers and managers in the course of their routine tasks. Reactive errors are those discovered as a result of investigation following an incident or another reported (proactive) error. An issue was raised if both types of errors would be recorded and if recording proactive errors would be penalizing, i.e. to the organization's image. Both types must be recorded to obtain a true performance state. Proactive errors are not penalizing. It is important that proactive errors are recorded, because in doing so the operator would accumulate credit for the effectiveness of its defence system as proactive error records are a manifestation of the organization's alertness to human error, and the quality of work output. Obviously any proactively detected errors would invariably be defended and would have no detrimental flight consequence; therefore, unlike a reactive error would do, effects of proactive errors would not feature in flight consequences other than as No Error.

6.30.4 Level 1 and Level 2 Findings

Usually Level 1 and Level 2 Findings are made by CAA Regulator. In the risk model a proactive finding can be considered a form of defence, because it would trigger an action to put matters right. This information is fed back to the AO immediately after the oversight, and should be available to them for inputting to the model. During validation trial, Regulator findings were provided by the operator itself. These errors would be recorded in the Compliance subsystem only

Shortcomings in compliance, discovered as a result of an investigation into an incident is a reactive input. However errors would be recorded under the relevant node in performance, and NOT in compliance subsystem. CAA had queried if retrospective finding of non compliance with regulation resulting from an incident investigation would reflect unfavorably on CAA's ability to undertake regulatory compliance oversight inspection. It cannot be considered so, because it is known that such inspections take on a snap-shot of the organization at the time, and that time dependent changes could occur. Besides, audits are usually spread over a 2-years period. At any one time, less than 100% of the auditable items would get inspected. Therefore it is perfectly acceptable to have compliance shortfall identified by the operator as a result of an investigation, without it adversely reflecting on the Regulator. If the error relates to a long period trend, then of course that would rightly raise a question about the relevant inspector's alertness and skill levels, or the possibility of his making errors. He too is human.

6.30.5 Weighting L1 and L2 Findings

CAA currently uses a weighting factor to discriminate between Regulation clauses according to their importance. This model does not allow weighting, and the concept has no facility. However, in a model that is driven by actual information on real events, it was considered that weighting has no significance. For instance, consider the case where there were two causal factors to an incident. Suppose that it was the less significant factor that led to the accident and not the more high profile causal factor. No matter how important a causal factor is in its own right, if it had not contributed to the known incident then there is no point in weighting it. Whatever the causal factor that contributed to an incident, would be recognized by the model, and the model would then show it in its marginal distribution list, as embedded within the node.

Weighting may however be considered as a influencing factor by the Regulator whenever they use the risk data provided by the model for follow up decisions, such as legal penalties, revoking a license or providing leniency. For this purpose, the Authority could maintain a "Look up Table" or similar administrative aid to complement the information stored in the model**.** Before setting the Table, it is best to examine through sensitivity analysis which causal factors have the most impact on risk. Sensitivity analysis will be explained in Chapter Seven, Working with Data.

6.30.6 Incidents under investigation

Errors and causal factors for those incidents under investigation would not be available until the investigation was completed. CAW Risk Model calculates for known data only, yet it is not advisable to ignore any "pending data". Therefore flights that have had errors, for which investigation findings have yet to be made available, would have to be "parked" in a separate area of the database and brought into the main database when all the necessary information is available. Meanwhile, they could remain in the parking area, and be visible to all concerned. It is a practical, administrative issue and does not affect the way the model computes the risk.

6.31 Combined Cost

This section provides an explanation of the design of the Combined Cost Node (Figure 6.13). This node provides information to undertake risk calculation, if risk is to be determined using the traditional formula:

Risk = Probability of the hazard occurring x severity of consequence. 6.1

The parameter "Cost" is used in general sense to indicate the monetary outcome of an error that is either discovered or missed. It includes the cost of putting matters right on discovering an error or of its consequences, regardless of the fact that it might be a part of the sunken cost, a new expenditure or an insurance payout. If error was missed and led to an incident, then the consequence could generate bigger costs, either to the operator or if not to its underwriter.

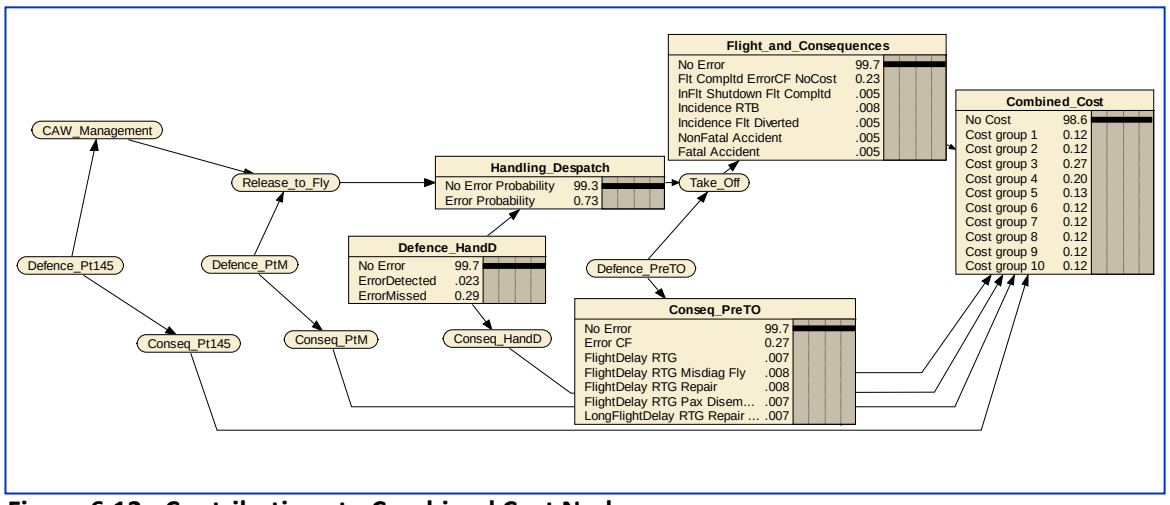


Figure 6.13 - Contributions to Combined Cost Node

6.31.1 Combined Cost node design

It should be noted that cost is a continuous variable, but in order to generate probability distribution it would have to be discretized, either at data gathering stage or if not at the processing stage. In this model, for simplicity of handling, cost has been discretized into Cost Groups at the data handling stage.

The node has 11 cost groups against which cost data can be recorded. These are labelled as “No Cost”, “Cost Group 1”, Cost Group 2” etc to “Cost group 10”. A monetary value is assigned to each group using a “log scale to base 10”. At present the monetary value of the lower end of the scale is zero and the upper limit is £10B, facilitating the recording of a full range of costs from a negligible cost of an inconsequential error to an extreme high cost of a disastrous consequence. It is recognized that lower end cost groups 1 and 2 and possibly 3 are of no significance; nevertheless they are retained here for completeness and to demonstrate the concepts.

In a real life application, lower cost groups could be truncated if necessary, and upper cost groups could be further subdivided to improve resolution according to the wishes of an operator. Moreover new groups could be added to identify even “profits to the operator” as it has been suggested by one operator that some accidents end up with profits (presumably as insurance payouts).

6.31.2 Cost contributions

Various contributors to the Combined Cost Node are identified in Figure 6.13, though it may not necessarily be the full picture. Costs arise from several sources, depending on if there was an error, if it was detected, or if it was missed. A detected error may be allowed to lapse, be carried forward or be corrected. A missed error might remain dormant or cause an incident. Delayed or cancelled flights, diversions, engine shut down in flight and accidents make large contributions to the cost.

Altogether there could be several thousand permutations based on the number of defences, whether an error was detected or missed, the outcome of a detected error or a missed error and the monetary gain or loss they could incur. When relevant information is input to an individual node, the software allocates the observed data to the most appropriate permutation.

6.31.3 Missed errors.

Consequence of a missed error that moves into the flight phase is recorded in the Flight & Consequences Node. This node has 7 categories of consequences, but it could be more or less according to the level of resolution required. The categories define varying severity of consequences, and range from "No Effect" at one extreme to a "Fatal Accident" at the other. Each consequence may have a monetary outcome according to its severity, varying from zero to £10B or more. The rank order of flight consequences is not matched to the rank order of Cost Groups, but they are mapped as permutations in a conditional probability table, i.e. 7 consequences and 11 Cost Groups produce 77 permutations.

6.31.4 Detected Errors.

If an error is detected, corrective action can range from no action, an investigation, to a near and far term solutions to prevent a recurrence, e.g. simple AMM amendment or fleet modifications. Putting right a detected error could vary from no cost at one extreme to several million pounds at the other extreme. Thus possible consequences of a detected error are linked with Cost Groups through different permutations.

6.31.5 Monetary value of consequence of error

Tangible costs. Only tangible costs can be collected, these being: material, labour and consequential losses. Consequential losses could be the cost impact on the operation, i.e. the business turnover, loss of aircraft availability, extra airport fees, hotel charges etc, as well as personal injuries.

Personal injury and fatalities. Cost of injury and fatalities have been considered to the extent what lawyers and insurers would agree on a monetary value to consequences of injury and loss of life and what law courts agree as reasonable. There are guidelines on how these figures are reached[116]. However this research study has refrained from estimating a compensating value either to loss of life or to preventing a fatality, or to injury or what a court might award. The study simply allocated a range of values to cost groups, which might be sufficient to cover any foreseen eventuality; it could be extended if necessary.

Intangible costs. Intangibles such as loss of reputation of the company, the cost of emotional suffering of the injured or of the relatives of the dead have not been accounted for. Again, the range of cost groups provided should be sufficient to record

losses due to a company going bankrupt resulting from loss of reputation and future business. A company going into liquidation might be a tangible cost.

6.31.6 Output from Combined Cost Node.

The output from the Combined Cost is the probability of the cost occurring in each respective Cost Group, based on the operator's performance up to that point in time when the relevant data was collected. The results could be used to calculate the risk. It may be noteworthy that the output from the combined cost node matches the definition of risk given by SMM at Section 3.3, i.e. the predicted probability and severity of the consequence(s) of a hazard taking as reference the worst foreseeable situation.

6.32 Risk output

At present the model does not provide a risk output as it is traditionally defined, i.e. the product of the probability of hazard and severity of its consequence. Instead the model provides a lot more information: the probability of causal factor (this being the hazard), the probability of error at critical points in the CAW process, the probability of the type of consequence and the probability of a certain cost arising resulting from the hazard. This is a much larger range of management information than a single-number risk value could provide. Thus a CEO/AM could have the "X" probability of a certain consequence given that the CAW process in his organization carries a human error probability of "Y" at the end of the process. Operators have expressed the view that this method of presentation was more beneficial to them than the use of a single number. If he can improve on "Y", then "X" will improve; thus safety management could be objective with a measurable result.

If a single numerical risk value is needed as a stand-alone parameter then it can be obtained as the (mathematical) product of the probability of Cost Group and the allocated monetary value to that Group. The lower limit of the cost group can be used; other interested parties could well use an upper limit, mean or a lower limit according to what they wish to promote. Since the Cost Groups were based on a log to the base 10 scale, there is a large differential between the upper and lower limits of the group. Therefore, at the end, interested parties should come to a common agreement, say, between an operator and an underwriter, on the required degree of resolution and a fair definition for the Cost Group.

Risk calculation was not included in the current configuration of the model as it terminated at the point of outputting probability values for each Cost group. A

subroutine for this function could be added during the development phase. Meanwhile for demonstration purposes, risk calculation was performed manually, outside the model.

6.33 Confidence on the structure of the model

Finally, on the question of how much confidence one could place on the model, a vital point to be made is whether the ID constructed is the "correct one" for the decision situation. In this regard, Clemen (2000)[85] (pp 67) offers important advice. He states that the question pre-supposes that a unique correct ID exists, and goes on to qualify by stating that this supposition is not true, because there are many ways in which an ID can appropriately represent a decision.

Clemen (2000)[85] offers guidance by stating that, instead of the correctness of the ID, one should consider if the ID is appropriate or not. He quotes Phillips (2000): "*Phillips (1984)[99] states that a model can be considered requisite only when (either) no new intuitions emerge about the problem, or when the model contains everything that is essential for solving the problem. That is when the decision maker's thoughts about the problem, beliefs regarding uncertainty and preferences are fully developed*". Clemen (2000)[85] further states that, *"A careful decision maker may cycle through the model several times as the analysis is refined, part of which will be doing sensitivity analysis. The only way to get to a requisite decision model is to continue working on the decision until all of the important concerns are incorporated"*

During the early stages of the research study many different attempts were made to arrive at an ID to represent the CAW process, error, consequence and risk, but they all failed until the earliest ID constructed that resembled the current family of ID (Figure 6.2). Since then there have been different evolutionary stages of the model. The one reviewed by CAA had the same subsystems as the present one, but it contained only 107 nodes (Figure 6.16). The current generic model has 178 nodes, whereas the model offered up for validation trial has been further modified to suit local conditions.

On the basis of the experience gained in this research study, the following advice is also offered to future researchers by way of a qualification to Clemen's guidance. The iterative process is a necessity in any model that has a heuristic root. It is certainly essential if structure learning from data precedes model design. Structure learning is essential if the process that is going to be modelled has had either no previous structure, or if a structure was present and dormant but it had not been recognized. To give an example of structure learning, learning the habits and patterns of motorists who criss-cross a region going to work in the morning or returning home would

require structure learning from data gathered, if that region has not been previously surveyed.

Fortunately this study did not require such structure learning, because CAW process in itself already had a structure. It is a process that had evolved from almost 100 years of experience in aviation; there is a large reservoir of knowledge and experience of this existing process, where a hierarchical and sequential order exists. The researcher's relevant knowledge and experience in industry has been used for setting up the initial structure, and the solution has been progressively stage reviewed by a panel of industry expert in order to gain consensus as these experts represented those who have the purview for CAW process audits in UK. Their comments and suggestions have been incorporated into the model, and in doing so the original layout has been revised iteratively.

Furthermore, the final, generic model has been presented to CHIRP/MEMS Steering committee, consisting of safety and quality managers from industry and specific aircraft operators who participated in the program. The solution has been well received by them before it was further offered up for validation using field data, which will be described later in Chapter Eight. A similar approach to iteration, based on industry experts' consensus, had been taken in the development of an MCDA/AHP type risk model by CAA-NL in which a fish-bone structure had been used to represent relationships between abstract qualities of an organization[62].

The current solution, in the form of this model, is more robust than any structure that would have been possible with computer based structure learning, because available error data for any one organization is insufficient to create a reliable structure.

That said it is necessary to reflect on the fact that the model is a generic model. Its application to a specific operator may well require minor amendments regarding certain nodes, without altering the fundamental structure, as it was the case when the model was used in the validation phase. If the generic model is going to be used for setting a bench mark for industry through a pilot study, then it would be necessary to agree on the structure of the model by all those participating in such a pilot study, if it were to be modified to suit the pilot study.

6.34 Air cargo subset

Addressing the needs of the air cargo community a subset of causal factors that contribute to risk to the safety of the aircraft has been designed. They fall outside the strict boundaries of CAW processes, usually falling into a domain straddling between CAW processes and flight operations. However human error in the course of

preparing the aircraft for its role could compromise the airworthiness of an aircraft that has already been certified as airworthy and has been released to service.

The subset takes into account errors attributed to conditions in the cargo loading environment, cargo loading operation and the state cargo has been restrained in the aircraft. Defences undertaken prior to certifying the load as fit to fly might or might not detect any errors. If they were detected, then there would be a consequence that could add a cost to the operation. If error was missed before the aircraft completed its Handling & Despatch, and if flight crew too missed noticing it, then it would be carried forwarded to the flight. The error could lead to an incident, or if not either it would remain dormant in the aircraft or dissipate with off-loaded cargo provided the hazard was confined to the cargo container.

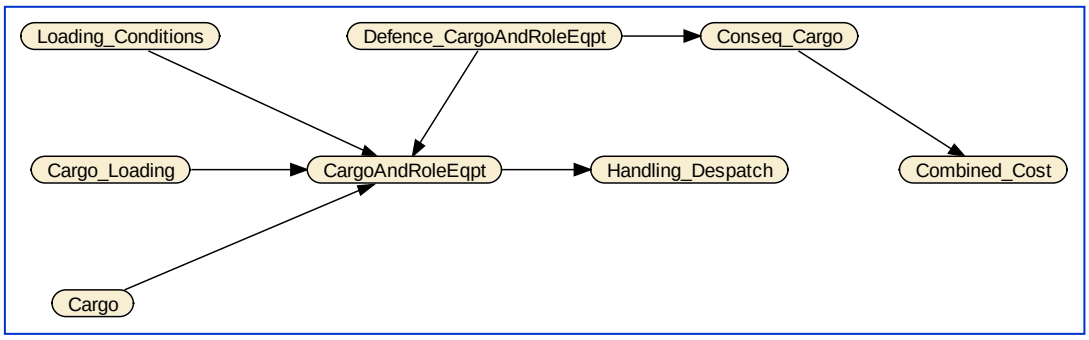


Figure 6.14 – Air cargo subset

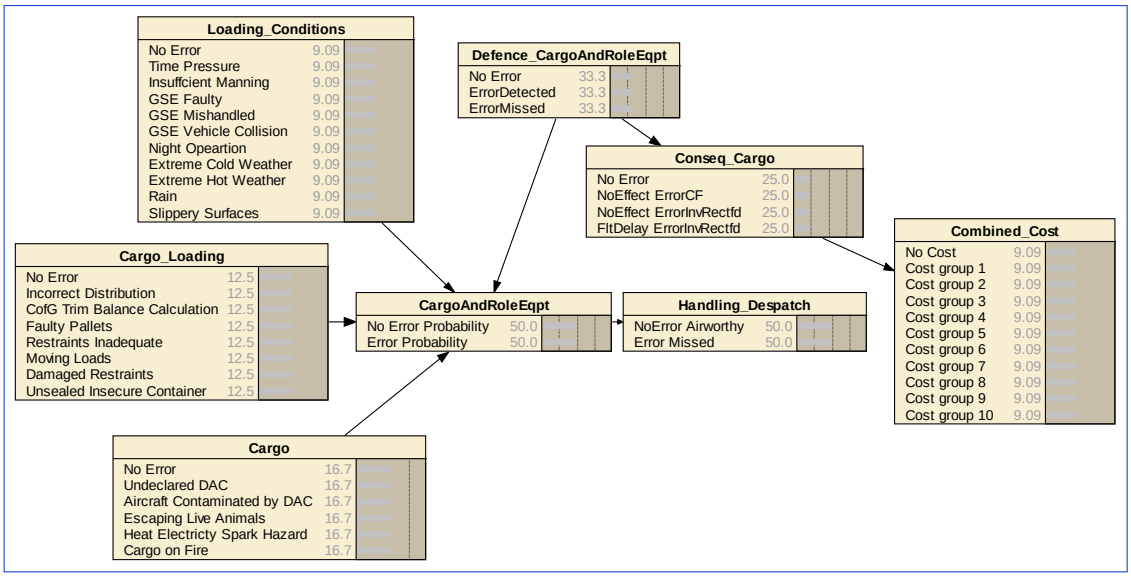


Figure 6.15 – Air cargo subset – Causal factors

Figure 6.14 provides the configuration of the BBN for the air cargo subset. Figure 6.15 represents the same configuration in the Belief Bar form, exposing the nodes and states of nature. Causal factors considered are tabulated as causal factors distribution, i.e. blank form and no data input. It shows equal probability distribution, i.e. no bias due to the absence of data.

The subset is intended to be grafted between the Handling & Despatch node and the Combine Cost node. Figure 6.18 represents the model when air cargo subset is included.

6.35 Output from this chapter

The principal outputs from the research work described in this chapter are:

- The model structure representing the hierarchical order of the CAW process, influencing factors, and the relationships between process events, errors, consequences and risk.

- Taxonomy of events, errors, consequences, causal factors, all embedded in relevant nodes of the model.

An electronic digital copy of the model with embedded parameters is in the accompanying CD; it requires a NETICA commercial software package to be installed in the computer, recommended Version 411 or later.

The next Chapter will describe how the model could be used with data.

Intentionally Blank

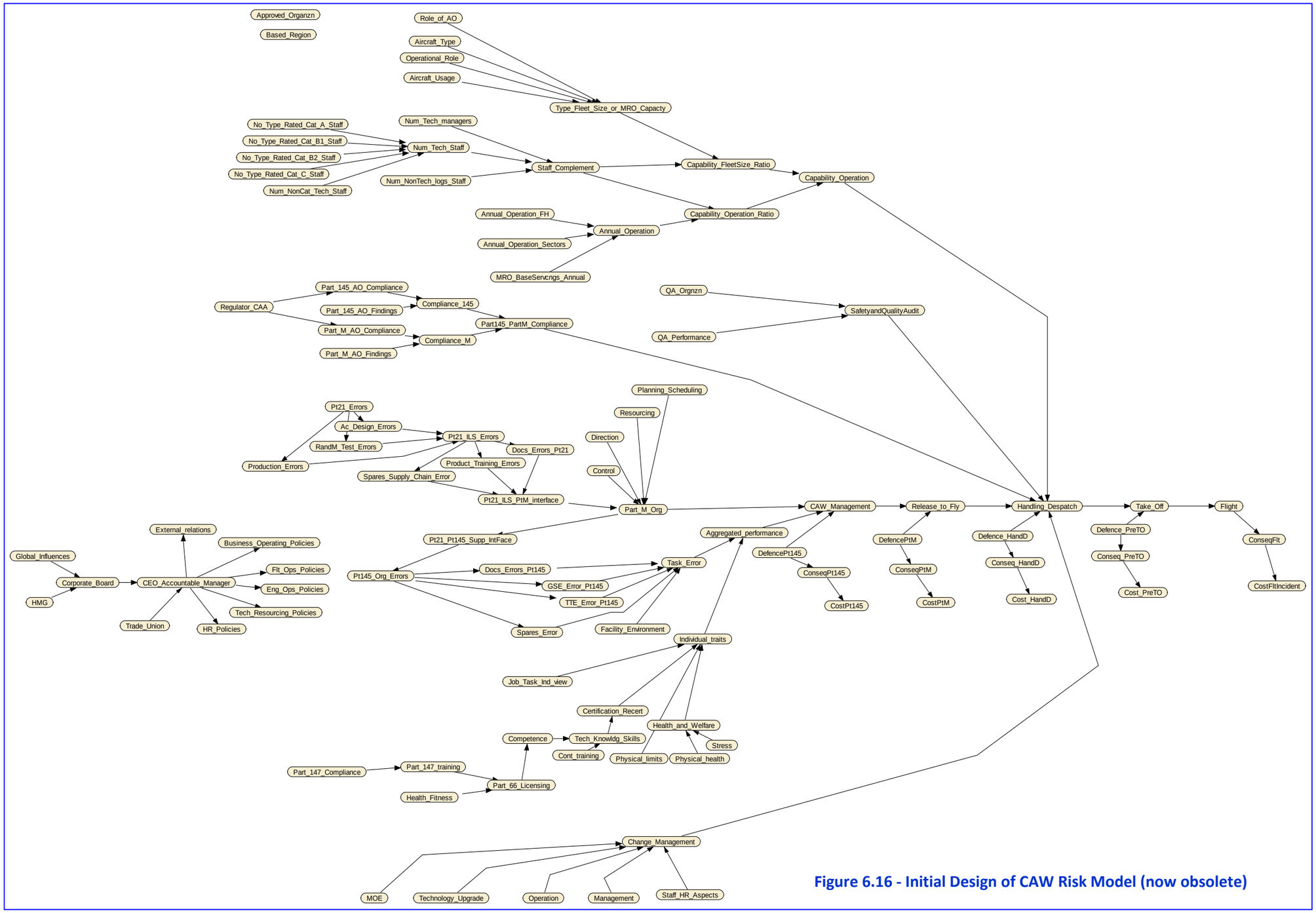


Figure 6.16 - Initial Design of CAW Risk Model (now obsolete)

Intentionally Blank

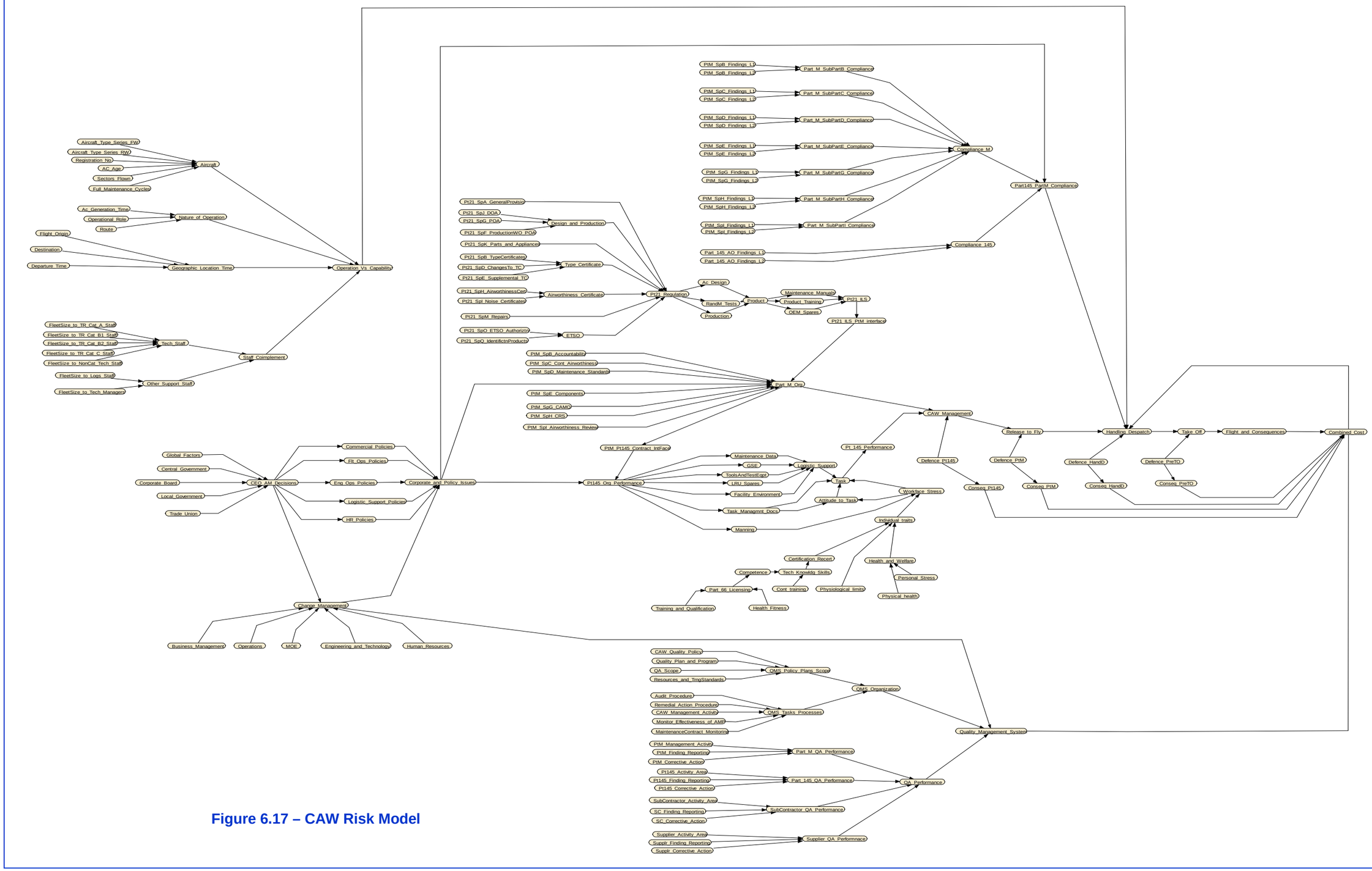


Figure 6.17 – CAW Risk Model

Intentionally Blank

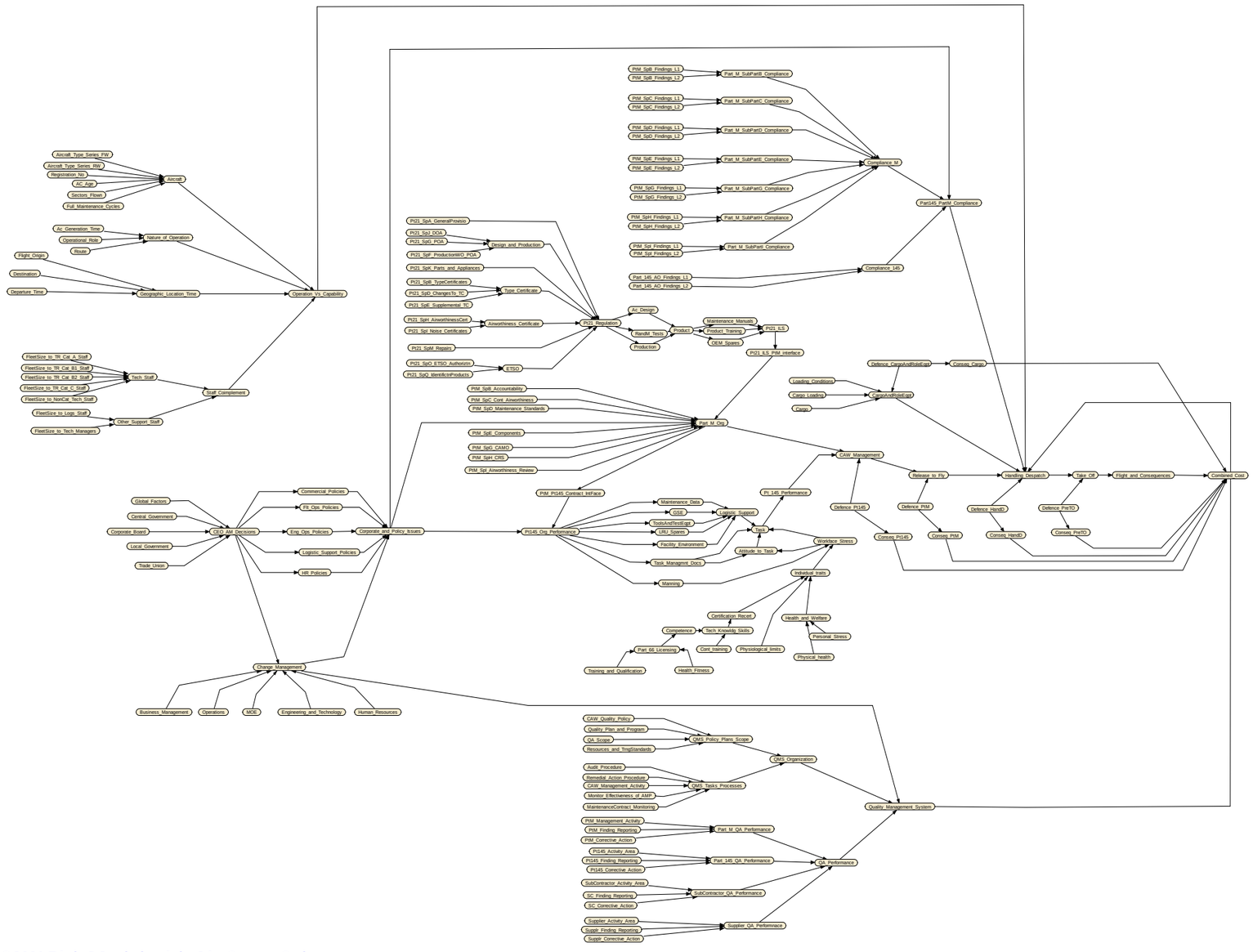


Figure 6.18 – CAW Risk Model with Air Cargo Subset

Intentionally Blank

Chapter Seven

Model – Working with data

7.1 Introduction

A high-level perspective of the role and types of data, and the way they fit into the risk assessment methodology was given in Chapter Six and in Figure 6.1. This chapter demonstrates how the model works with data. It will discuss the procedures followed for data preparation, their uploading to the risk model and then, the way tests were conducted to confirm that the model was working satisfactorily.

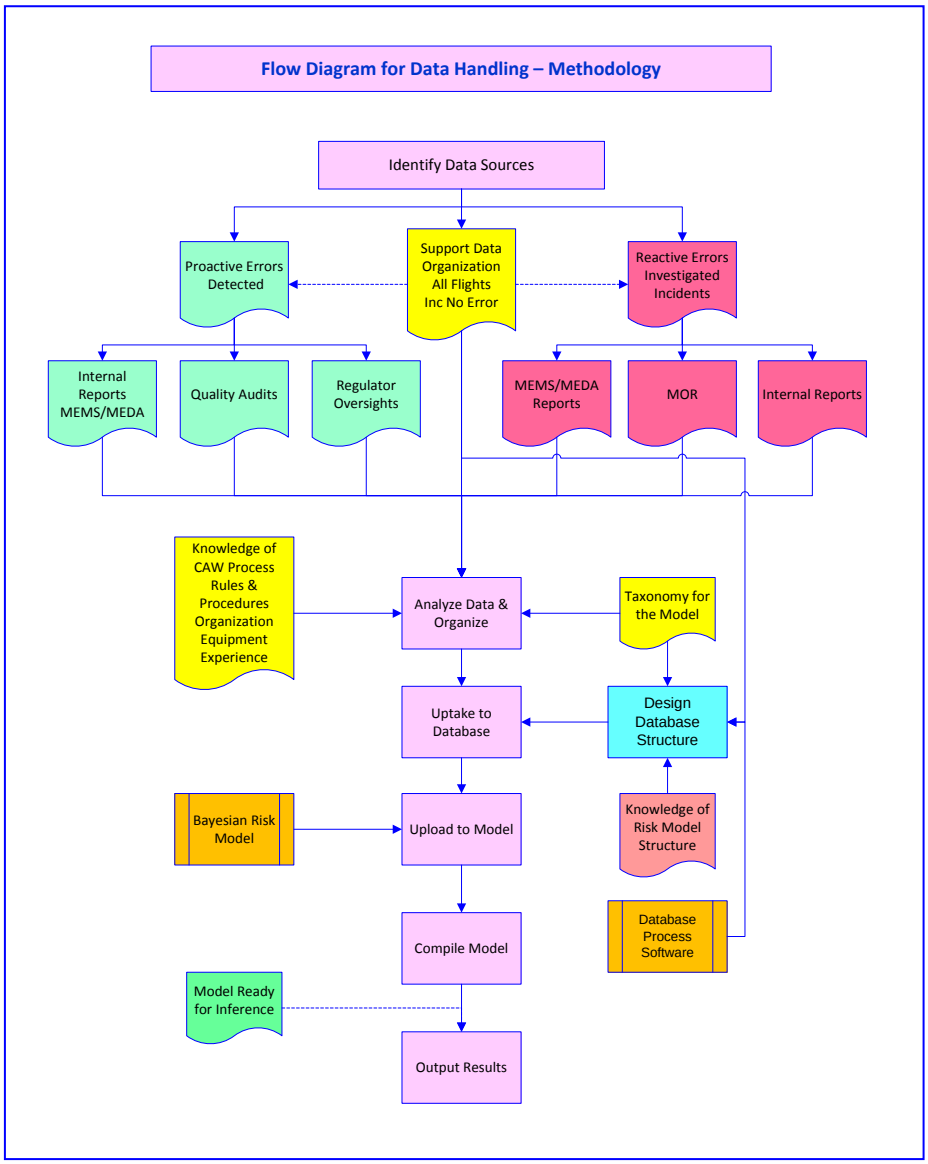


Figure 7.1 – Flow diagram for data handling

7.2 Overview of data handling

7.2.1 Raw data

The risk model needs data from error free flights as well as data on errors that occur in the organization and human/ aircraft interface during the implementation of CAW process. Proactive error data as well as reactive error data are used. They are available in various reports of investigations carried out on reported errors, ground and flight incidents, quality audit and the Regulator oversight inspection "Finding" reports. These reports may contain information that have been already analyzed, and probably categorized, by subject experts for different technical management purposes.

Proactive error data comes from detection during routine CAW process activities, or associated support activities; findings from Quality Audits and the Regulator oversight inspections are also categorized as proactive for the purpose of this model. Reactive error data comes from investigation of incidents.

All this information collectively constitutes raw data for the purpose of risk assessment. To use this data in the CAW risk model they should be converted and transferred to a digital database.

7.2.2 Data analysis

First, raw data should be analyzed and reorganized to a form that is usable for risk assessment, taking into account the defined taxonomy for the risk assessment model. This task can be handled by a subject expert only, as it requires a full comprehension of CAW process, rules and procedures as well as considerable knowledge and experience of various subjects: aircraft engineering, maintenance and integrated logistic support, aircraft type and associated equipment, organization management and human factors to name a few. These analysts must know what the required standards ought to be in CAW processes and its management, and industry best practices to ensure the airworthiness of an aircraft.

7.2.3 Database

There should be a purpose designed database to uptake analyzed and reorganized data, and to retain them for use as required. In this occasion a spreadsheet has been used for this purpose. The spreadsheet should be designed using proprietary database software, such as Excel or Access; this study used Microsoft Excel. Prior knowledge of the taxonomy for the risk model and of the risk model structure is necessary to undertake this work.

7.2.4 Operating model with data

When the spreadsheet template is ready, analyzed data could be transferred to the spreadsheet, progressively building up the database. In the next step of data handling, data from the database containing several thousands of flights could be uploaded into the model as a batch file, and then compiled. NETICA User Guide[90] provides instructions on the correct procedure, and then how to compile the network.

A compiled model displays the risk status of the organization linked to the point in time to the last input data set. If it is reasonably close to the current time period, then it could be used as indicative of the current status of the organization. With new data input, the status would change, but in practice the rate of change may be imperceptible under normal steady safe conditions. However new error findings at sensitive nodes could make noticeable differences to the risk level.

Initial results output by the model are called prior probabilities at each node. At this point the model is ready for drawing inferences and other uses, e.g. to determine implications of a new error finding at an upstream point in the CAW process on the error probability at a critical node such as Handling & Despatch. Response to a finding is called posterior probability. For example, a result may be expressed as, “given prior probability, if a new error finding was at Task node, then the posterior probability of error at Handling & Despatch would be (X) per cent”. X is the new value output by the model.

7.3 Database spreadsheet

Using information from the raw database, a data file should be prepared either in Excel or Access spreadsheet. This will be the database for the model.

Columns of the spreadsheet carry the names of nodes of the BBN. Embedded within the nodes are States of Nature for each node.

The nodes and states of nature have already been pre-defined in the taxonomy used for the model, as listed in Appendix 10 and Appendix 12. The column headings for the spreadsheet follow the same pattern, and same order.

Drop down menus designed into the matrix under each node (or column heading) enable the operator to select the most relevant information from a multiple choice of states of nature. A specimen of such dropdown menus is shown in Figure 7.2. Full set of drop down menus is in Appendix 12.

Part_145_AO_Findings_L1	Part_145_AO_Findings_L2	Compliance_145	PtM_SpB_Findings_L1	PtM_SpB_Findings_L2
No_Error	No_Error	No_Error_Probability	No_Error	No_Error
A20_Terms_of_approval	A20_Terms_of_approval	Error_Probability	MA201_Responsibilities	MA201_Responsibilities
A25_Facilities	A25_Facilities		MA202_Occurrence_Reporting	MA202_Occurrence_Reporting
A30_Personnel	A30_Personnel			
A35_Certifying_and_suppt_staff	A35_Certifying_and_suppt_staff			
A40_Tooling_Material_Eqpt	A40_Tooling_Material_Eqpt			
A42_Acceptance_of_components	A42_Acceptance_of_components			
A45_Maintenance_data	A45_Maintenance_data			
A47_Production_planning	A47_Production_planning			
A50_Certification_of_maintenan	A50_Certification_of_maintenan			
A55_Maintenance_records	A55_Maintenance_records			
A60_Occurrence_reporting	A60_Occurrence_reporting			
A65_Safety_and_Quality	A65_Safety_and_Quality			
A70_MOE	A70_MOE			
A75_Privileges	A75_Privileges			
A80_Limitations_of_AO	A80_Limitations_of_AO			
A85_Changes_to_AO	A85_Changes_to_AO			
A90_Continued_validity	A90_Continued_validity			
A95_Findings	A95_Findings			

Figure 7.2 – Specimen drop-down menus for mapping State of Nature data

Using this arrangement now it is possible to prepare a template spreadsheet to accept analyzed data. The first row of data could be set to either “No-Error” or “No-Error-Probability” as the case may be from each drop down menu. Then by selecting the first row of data and dragging down to cover as many rows as desired a large spreadsheet could be initialized with “No Error” data. That means all potential CAW process cycles/flights, where there would be no errors, would have been already uploaded. This initialization of the spreadsheet should not be construed as an incentive to avoid recording data; it is a facility to minimize the effort for recording “No Error” data that might be perceived as an unproductive task. With a pre-initialized spreadsheet the organization simply tracks progress of CAW process/ flight cycles for each aircraft that goes through the organization, and enters only error data when they do occur. It is a very simple operation, and maintaining the spreadsheet is a very low cost task in man-hours.

The spreadsheet carries row numbers on the extreme left end column. Rows of the spreadsheet, line by line, represent successive flights launched by the organization in a chronological order together with the CAW process started from the end of the previous flight. The CAW process cycle starts on the aircraft’s arrival at the gate and finishes on departing from the gate. The flight phase follows on after departing from the gate and terminates on arrival at the destination’s gate. That is the full cycle. The cycle is repeated, and each row of the spreadsheet represents this full cycle.

In addition to the row numbers, an organization could record other management information such as aircraft registration number, flight identification, location etc, which would help to track the progress of organizations flight operation activities. However if there are no errors, the risk model does not need this data. They must NOT

be uploaded to the model; they can be retained in separate non-active columns for local management purposes. In a more developed commercial model this type of separation could be undertaken by programming the software for user interface.

Thus a full database should contain Error and No-Error information on all the flights launched by the organization and its preceding CAW process. A portion of the completed spread sheet is presented in Figure 7.3. A full spreadsheet can be found on the attached CD, File titled: *Combi 5_All_Cer2_data for txt file* in the Folder titled, Integrated Model. Note that drop down menus are usually disabled in a text file.

IDNum	PtM_SpH_C	PtM_Spl_Air	PtM_Pt145_	PtM_Pt14	Pt145_Org_I	Maintenan	GSE	ToolsAndTe	LRU_Spares	Facility_En	Logistic_Su	Task_Mana	Manning	Attitude_to	Workface_S
1	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
2	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
3	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
4	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
5	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
6	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
7	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
8	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
9	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
10	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
11	No_Error	No_Error	Contract_cor	Error_Probal	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
12	No_Error	No_Error	No_Error	No_Error_P	A45_Mainte	Not_updated	No_Error	No_Error	No_Error	No_Error	Error_Probal	No_Error	No_Error	No_Error	No_Error
13	No_Error	No_Error	Contract_cor	Error_Probal	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
14	No_Error	No_Error	No_Error	No_Error_P	A40_Tooling	No_Error	No_Error	Unreliable	No_Error	No_Error	Error_Probal	No_Error	No_Error	No_Error	No_Error
15	No_Error	No_Error	No_Error	No_Error_P	A25_Facilitie	No_Error	No_Error	No_Error	No_Error	Other	Error_Probal	No_Error	No_Error	No_Error	No_Error
16	No_Error	No_Error	No_Error	No_Error_P	A45_Mainte	Poor_access	No_Error	No_Error	No_Error	No_Error	Error_Probal	No_Error	No_Error	No_Error	No_Error
17	No_Error	No_Error	No_Error	No_Error_P	A45_Mainte	Poor_access	No_Error	No_Error	No_Error	No_Error	Error_Probal	Inaccessible	No_Error	No_Error	No_Error
18	No_Error	No_Error	No_Error	No_Error_P	A45_Mainte	Poor_access	No_Error	No_Error	No_Error	No_Error	Error_Probal	Inaccessible	No_Error	No_Error	No_Error
19	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
20	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
21	No_Error	No_Error	No_Error	No_Error_P	A30_Personr	No_Error	No_Error	No_Error	No_Error	No_Error	Error_Probal	No_Error	No_Error	No_Error	No_Error
22	No_Error	No_Error	No_Error	No_Error_P	A30_Personr	No_Error	No_Error	No_Error	No_Error	No_Error	Error_Probal	No_Error	No_Error	No_Error	No_Error
23	No_Error	No_Error	No_Error	No_Error_P	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Pr	No_Error	No_Error	No_Error	No_Error
24	No_Error	No_Error	No_Error	No_Error_P	A40_Tooling	No_Error	No_Error	Poor_Contro	No_Error	No_Error	Error_Probal	No_Error	No_Error	No_Error	No_Error
25	No_Error	No_Error	No_Error	No_Error_P	A40_Tooling	No_Error	No_Error	Unreliable	No_Error	No_Error	Error_Probal	No_Error	No_Error	No_Error	No_Error
26	No_Error	No_Error	No_Error	No_Error_P	A42_Accepta	No_Error	No_Error	No_Error	Other	No_Error	Error_Probal	No_Error	No_Error	No_Error	No_Error

Figure 7.3 – Portion of the spreadsheet

7.4 Data capture

Rules for data capture had to be devised as the study progressed. This section discusses the experience gained, though by no means it is an exhaustive set of rules. The listing is not in any particular order. The following data capture method is principally applicable to an AOC Holder with an integrated Part M and Part 145 organizations, and outsourcing en-route maintenance support from a third party contractor.

7.4.1 General guidelines on data capture

Data should be recorded for every aircraft operated by AOC Holder, for every CAW process cycle/ flight. To enable this, a row in the spreadsheet is dedicated to the CAW process cycle/ flight.

If there were no errors reported or discovered, nor any error related incident, then the row should record No Error data in every cell in the row.

If an error was reported or detected, then relevant data should be recorded in appropriate cells in a row.

Flight or aircraft identification information should be recorded in relevant cells, only when an error has occurred. If there were no errors, then this type of management information must NOT be recorded as model input data.

If there is an error input, then the causal factor for that error should be recorded in the relevant node. All other relevant information should also be recorded under each node, if known. Relevant information to be recorded could be selected from the drop down menus. Only prescribed selections could be made; terms made up by the user would not be accepted.

"No Error" data is accountable. If a node registers No Error, then it is called "No Error" data. If there is no error, then each node of the spreadsheet would uptake "No Error" data. If the spreadsheet has been already initialized with "No Error" data, then the information is already there in position.

All nodes in a row must be completed with either No Error data or Error data. If there is no information, or data not known then it is best to input a No Error against the node; the assumption is that the event/node concern has not contributed an error; it gives the organization the benefit of doubt.

Consequences are based on the actual outcome of the flight and NOT on a worst foreseeable scenario as ICAO SMM Chapter 5 "Definition of Risk "suggests[29, 38]. The final outcome of the CAW process would be known only after the aircraft has arrived at the gate of the destination. Until the outcome is known, data entry activity on the row should remain open, and at that point it should be closed after entering the final set of Flight Consequence and Combined Cost data.

7.4.2 Quality audit and Regulator oversight Findings

Errors detected during quality audits or as findings from Regulator oversight inspections are recorded on a row placed at a chronological order, matching the date of finding. If it is not related to a specific aircraft, such as a general organizational issue, then the record would be entered as an imaginary pre flight CAW process in order to take this information into the database. This technique might not be strictly accurate, but it has been devised in order to take into account the positive contribution from this defence, because invariably a Finding would lead to an in-house

improvement of the CAW process or organization. Any inaccuracy due to the introduction of “phantom flights” would be negligible.

7.4.3 Multiple causal factors in one node

A node should record only one selection at any one time, i.e. either a No Error or if there was an error, the causal factor. Only one causal factor must be recorded at any one time. If more than one causal factor is possible, record only the most important and relevant causal factor.

If it is essential to record a second causal factor, then allocate another row number, as if generating a “phantom flight”.

7.4.4 Incidents under investigation

Database work assumes that causal factor investigation has been done in each pro-active or reactive case. During this research study, existing already completed investigation reports were used as raw data. But in real life, there could be a phase lag between availability of causal chain investigation results and the incidence of the error line. Meanwhile it may be necessary to “park” the relevant row, until data is available. The record should be completed, closed and moved to the main database after its completion when investigation results are available.

It is assumed that, there will be an urgency to complete investigations promptly if this type of error recording under a new risk assessment concept is adopted by industry. It is acknowledged that in the present system, there is some laxity in getting investigations completed promptly.

The “parking area” concept would prevent the corruption of database, say, due to forgetfulness and missing information, or undermined importance due to time delay.

7.4.5 Relevancy of data and consistency

All data must come from one identified organization, if it is necessary to assess the risk contribution from one organization, like maintenance provider. If it is an operator, i.e. AOC Holder with an integrated Part M and Part 145 AOs, then the risk contribution is from the operator and their operation.

If an operation involves more than one organization, the sectors flown and errors or incidents for all aircraft that fell within the operation should be included regardless of the fact at which location they originated. This is because the aircraft operator, AOC Holder, is responsible for the airworthiness of the aircraft; how they achieve it, say, by either using its own Part M and Part 145 AOs or if not out-sourced organizations is

immaterial to the model. The model assesses the risk contribution from the AOC Holder's CAW process operation. There is a node for location data, and that will pick up intelligence of out-sourced services, so that the AM/ CEO could effectively manage that service according to their performance.

However if risk contribution from one named organization based at one location is considered, such as an MRO, then data should relate to all aircraft handled by that organization irrespective of the fact to which AOC Holder the aircraft belonged. This is the case when an AOC Holder has its own Part M and Part 145 organization at one location. These AOs may handle own in house aircraft as well as any visiting aircraft. Data relating to all handled aircraft should be recorded in the database relevant to the organization. This way, it is possible to ensure that there is a consistent data set for the organization, on which risk assessment could be made.

7.5 Uploading data into the risk model

The spreadsheet in Excel or Access should be converted to a text file before it is uploaded on to the risk model. Following uploading, the model should be compiled and this gives a model that has been primed. NETICA User Guide[90] provides Instructions for uploading data and compiling the model.

7.6 Inference

The primed model displays the status of the organization. This information could be obtained by studying each node of interest. The information contains "Prior Probabilities" for the organization, based on the period of operation to the point at which data was collected.

The model is also ready for inference, or interrogation. For example it could provide posterior probabilities in response to a finding in any one node or a series of nodes that represent a system failure. But before advancing to such tasks, it is necessary to get familiar with the displays, and undertake testing to see if the model behaves sensibly.

7.7 Nodes and "State of Nature"

In the graphical display of the model, each node (of a NETICA based BBN) is presented as a labelled box, with its name displayed. By clicking the mouse on the box, the node opens up to reveal a drop down window.

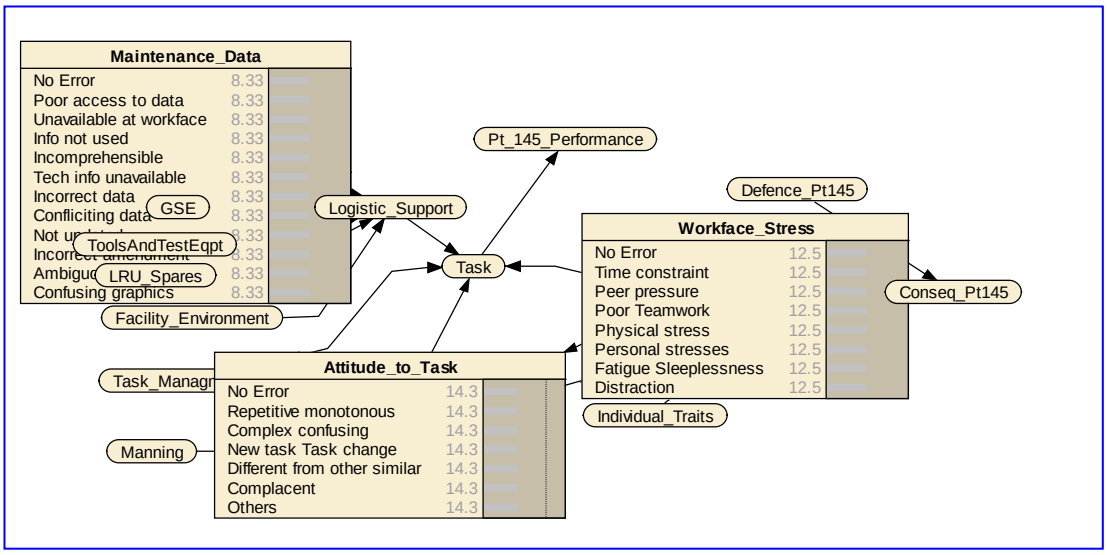


Figure 7.4 – Nodes and States of Nature – Equal marginal probabilities

7.7.1 Pre-initialized values – equal probabilities

Figure 7.4 is an example of nodes in open form, designated in the style of "Belief Bars". This portion consists of some elements from "Part 145 AO Routine Performance" subsystem. The example demonstrates the state of nodes prior to uploading of data, i.e. pre-initialization state of the model. In each box there is a listing of states of nature. For example, "Workface Stress" is considered as an "element level" influencing factor on risk, as it contributes to human error. Here the contribution attributed to Workface Stress could naturally exist in one of eight states: if there is no stress hence No Error, or if there is an error, then it could be in one of the seven remaining states; these seven are the possible causal factors that caused the stress. It may not be an exhaustive list of states, but this is the list specified by the taxonomy which is based on experience.

If new evidence reveals that the states of nature is limiting, then they should be amended by incorporating the new state. That would require a program change and perhaps a perceptible change of risk level as a result. Therefore it is a task for a Bayesian modelling specialist and not for the typical aircraft engineer, unless he has been trained in BBN skills.

Returning to the demonstration above, if there is a possibility of a state, then there must be a numerical probability of it happening. The numbers at the right hand side of the box are the numerical probabilities, here given as per cent. Here the indication is that they display equal probabilities. That means, if there is no data or any other knowledge of the behaviour of the parameter, the program assumes that all the states of nature could have an equal probability of occurring. These are marginal probabilities if nothing is known about their behaviour. If nothing is known about the

behaviour, then it is the most reasonable assumption. However as data is accumulated the probability distribution will display bias.

It can be seen from the boxes for the remaining nodes in Figure 7.4 that the marginal probability value can vary according to the number of states of nature in each node. Yet they all add up to 100%, allowing for rounding errors and truncation of decimal places in this display. The value 100% represents the certainty of something happening, either error or No Error put together, that is the total probability or the area under the graph if the situation is represented as a probability density curve. A new finding in the node, as used when interrogating the model for "what-if", would be indicated by a 100% probability against the relevant state. That is because a new finding is a certainty that there is an error. No matter how many states are there, if a state has been identified as a possibility, then there will always be a probability of it occurring, no matter how small it is. That is the way nature is.

There is an important lesson to be learnt, when it comes to the Flight Consequence node. If a catastrophic accident has been identified as one possible flight consequence, then in the calculations, there will always be a small margin of probability for it to happen, sooner or later, as a classical risk analyst would say. Experience, and therefore data, will eventually show if there is a bias.

7.7.2 Prior probabilities subject to data input

In comparison, Figure 7.5 demonstrates the states of nodes, after the model has been uploaded with experience (i.e. data) and compiled.

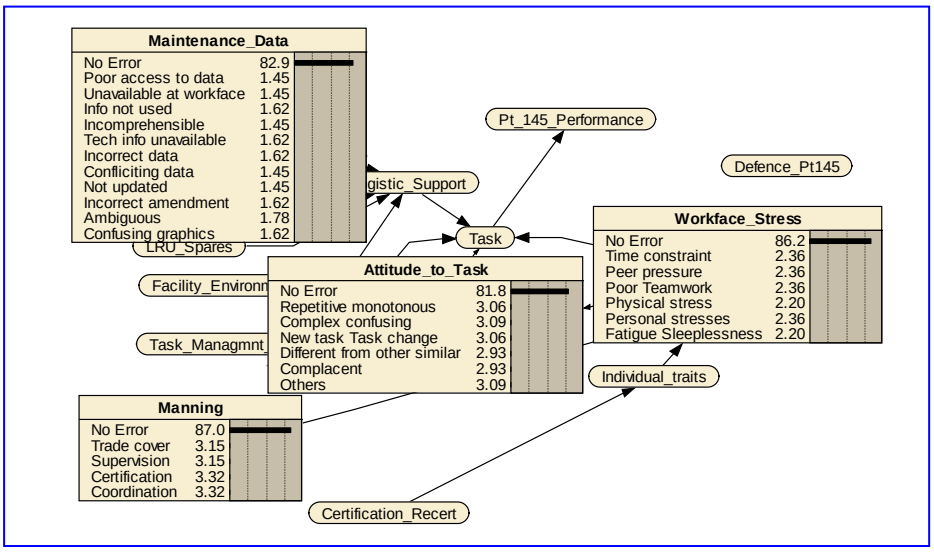


Figure 7.5 – Nodes and States of Nature - Output

Data input to the model accumulate in each node as they have been assigned. On compiling, the node displays the results in belief bars, and the distribution list gets updated, showing bias. Again, this portion of the model is from the Part 145 AO of "Routine Performance" subsystem. The results displayed here are from a simulation, and not real data.

This time, the numbers at the RHS of the tabulation indicate the probability distribution of causal factors for errors at that node in a given population as well as "No Error" (i.e. satisfactory) events. As anticipated, simulated "No Error" data has the highest percentage in the probability distribution, with varying levels of probabilities of other causal factors for errors occurring. These are the marginal probabilities (or prior probabilities) for this node, based on the population from which data came. It follows therefore that as more and more experience is gained, as more data is added to the database, the knowledge on the behaviour of the nodes, as well as of others, improves.

This demonstration underscores the value of recording No Error flights/CAW process cycles. This is because, in a reasonably safe operation, there is bound to be a much faster accumulation of error free CAW process/flight cycles than those, which had error reports. The distribution of probability for No Error and error flights would then becomes more representative, and recording of No-Error flights is beneficial to the organization in reflecting its performance.

7.8 Guidance on testing

Before using the integrated model with data, it was necessary to establish what tests were to be done on the model to ascertain its integrity. Literature research failed to yield any definitive information on tests, except guidelines provided by Clemen (2003)[85] that has already been discussed in Chapter Six (Section 6.33). It seems that guidelines on standard tests on BBN integrity do not exist, and there appears to be a gap in the knowledge as public domain literature currently stands. This query was referred to an experienced BBN practitioner who had once been a member of the Genie and Smile BBN software development team, who has substantiated that there were no standard tests, and that sensitivity analysis served this purpose, at least partially.

In the absence of specific guidance, the following check list is proposed based on the practical experience gained from this research study. The BBN should be reviewed to ascertain if:

- Logic of the influence diagram is correct.

- D-separation exists, between multiple parents' nodes that feed into child nodes.
- Architecture is complete.
- The BBN would compile properly when uploaded with data

It was already explained in Chapter Six that parts of the model, in subsystem form, were tested to ensure that they have been correctly constructed.

The most common errors were in spelling and syntax, or not observing the general rules for handling the software program at the construction stages. These types of error showed up immediately, as the construction could not proceed without correcting them immediately; others show up during compiling.

7.9 Testing subsystems using a specimen database

It was reported in Chapter Six, that each subsystem was tested for integrity before the subsystems were integrated into the model.

Node	No of errors	Row numbers	Causal factor
Pt21 Regulation	3	110 55 65	2 2 2
Ac Design	2	60 178	7 2
R and M Test	1	116	4
Production	3	58 90 193	2 2 2
Product	2	13 84	3 3
Maintenance Manuals	17 + (2)	125 19 126 132 183 40 105 110 163 64 143 176 15 73 92 72 76 174 197 + (159 69)	2 2 7 6 3 5 2 8 6 4 6 4 5 4 3 6 7 3 8 + (5 8)
Product Training	12	175 131 123 168 101 181 191 136 1 42 79 76	3 3 4 2 2 2 4 3 3 2 3 2
OME Spares	4 + (1)	192 64 7 77 + (179)	2 4 6 4 +(4)
Pt21 ILS	7	21 162 49 108 112 139 173 + 159 179 69	2
Pt21 ILS PtM interface	3	144 158 59 + (159 179 69)	4 7 2 + (9 7 9)
Planning Scheduling	9	115 156 74 165 143 200 148 26 160	4 4 8 6 7 8 7 4 5
Resourcing	13	107 130 93 128 59 75 125 97 149 33 89 67 190	4 3 7 7 4 3 3 6 6 7 5 4 7
Direction	2	50 171	5 3
Control	25 + (3)	96 68 49 62 157 35 53 87 43 164 103 57 84 121 33 170 4 199 106 72 91 40 24 107 141 + (179 159 69)	4 4 5 5 3 2 2 3 2 3 2 2 5 3 6 3 2 6 5 5 4 4 2 4 4 + (5 4 6)
Part M Org	12 + (2)	147 92 155 (179) 139 59 2 50 63 4 184 48 + (159 69)	2
PtM Pt145 Contract Interface	14 + (3)	34 76 154 96 59 142 152 6 182 57 74 132 48 78+ (159 179 69)	3 4 6 2 2 6 2 7 5 3 6 4 3 3 + (6 2 6)
CAW Management1	5 + (3)	154 31 155 120 137 + (159 179 69)	2
Release to Fly	3	159 179 69	2

Table 7.1 - Testing performance net - Part 21 and Part M elements

Each subsystem was tested by uploading simulated data to ensure that they compiled properly and to check if they produced meaningful results. Errors discovered during this process were corrected through modifications to the network. Data used in these trials were simulated using a random number generator, to identify the rows (representing CAW process /flight cycle) where errors occurred out of a limited population (201 rows). The number generator identified the row numbers and causal factors. A specimen error table simulated this way is presented in Table 7.1. The numbers in brackets identify those errors associated with system failures; they have been bracketed to assist tracing.

The data is for testing the Routine Performance subsystem for Part 21 product support elements together with associated contractual interfaces between Part 21, Part M and Part 145 organizations, represented by BBN in Figure 7.6**.**

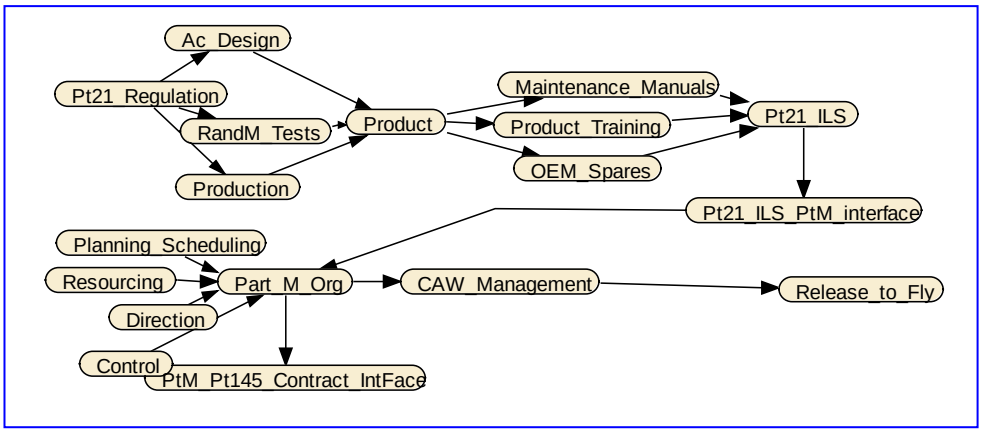


Figure 7.6 – Part 21 Routine Performance subsystem

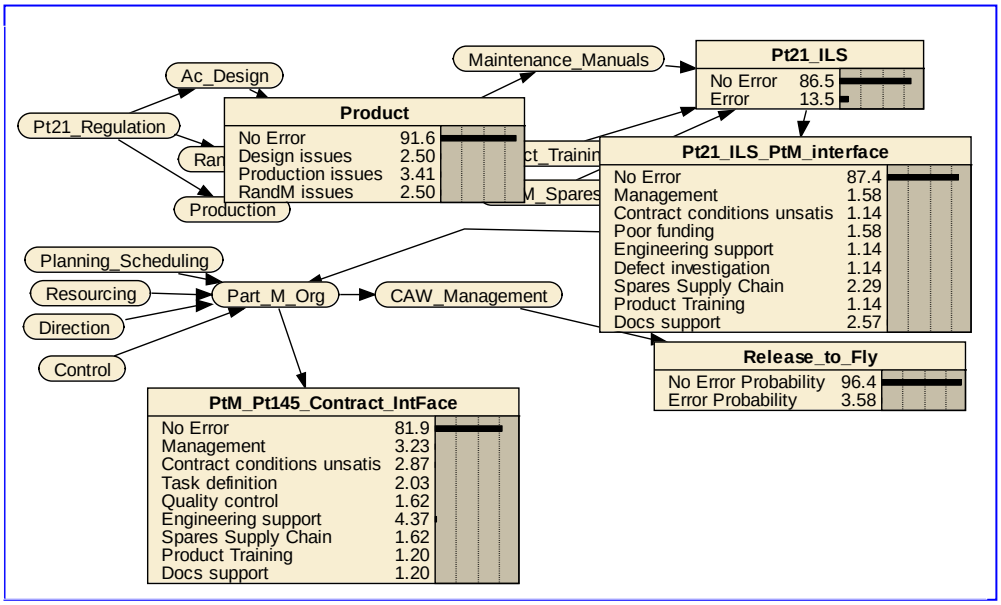


Figure 7.7 - Part 21 Performance - Support Contract Interfaces

This dataset was transferred to a spreadsheet, uploaded and compiled to give prior probabilities; prior conditional probability values for few nodes in the form of belief bars are presented in Figure 7.7. Only some of the nodes have been exposed for demonstration purposes in order to reduce clutter.

Values of prior probability at each node, for No Error condition, are tabulated in Table 7.2. The only way to test the accuracy of the results is to manually calculate them, as it was done in Chapter Five, Section 5.11.9. In this situation, attempting a manual calculation is unreasonable because it is very complex and impractical. For example, CPT for Part M Org node contains several hundred combinations of parent and child nodes' parameters; it is this complexity that drives BBN applications to be computer based. However, this situation posed a challenge, "How does one know that the program is calculating correctly?"

Node	Num of errors	Num of No-error	No error Flat rate %	No error Conditional Prior Probability %
Pt21 Regulation	3	198	98.5	98.0
Ac Design	2	199	99.0	94.5
R and M Test	1	200	99.5	97.2
Production	3	198	98.5	97.6
Product	2	199	99.0	91.6
Maintenance Manuals	17 + (2)	182	90.5	80.8
Product Training	12	189	94.0	87.8
OME Spares	4 + (1)	196	97.5	89.2
Pt21 ILS	7	194	96.5	86.5
Pt21 ILS PtM interface	3	198	98.5	87.4
Planning Scheduling	9	192	95.5	92.3
Resourcing	13	188	93.5	90.9
Direction	2	199	99.0	94.8
Control	25 + (3)	173	86.1	84.1
Part M Org	12 + (2)	187	93.0	82.1
PtM Pt145 Contract Interface	14 + (3)	184	91.5	81.9
CAW Management	5 + (3)	193	96.0	92.2
Release to Fly	3	198	98.5	96.4

Table 7.2 – Comparison of prior probability at nodes for No Error – Part 21 Performance

Literature research did not reveal a definitive answer to this question; Clemen (2003)[85] responded to it qualitatively but not quantitatively. In this study, it has been shown in Chapter Five, Section 5.11 that NETICA's calculation of conditional probability is accurate for a small group of nodes. In that case the next step is to consider if this accuracy is carried forward through the network. Contemplating on this problem, a rule of thumb method emerged that can be used to gain confidence; it

is done by observing the pattern of behaviour of prior probabilities propagating downstream as they interact with error observations in relevant downstream nodes.

The pattern was initially detected as a visual observation, and subsequently noted that it can be demonstrated as follows. Table 7.2 provides prior conditional probabilities, as well as the flat rate probabilities for the same nodes, based on the number of errors/ no errors observed against a base of 201 CAW process cycles/ flights (i.e. the number of rows in the database). In order to observe the pattern better, no-error counts, flat rate probabilities and conditional probabilities have been plotted on a graph at Figure 7.8. Flat rate probability values for each node have been used as a reference, because it can be easily calculated manually. Once, the pattern was set for the flat rates, one can observe how conditional probability values propagate through the network relative to the reference flat rate. X-axis scale automatically set by Excel only for the comparison of patterns, and not for reading the values.

It can be seen how the flat rate varies in response to variations of No-Error counts, but it is more interesting to observe that the conditional probability values vary in harmony. In this case it can be seen that the relative deviations of conditional probability values from the reference line on the graph are larger than the flat rate values. This behaviour is consistent and there are no glitches or sudden jumps to excessive peak or trough values that would possibly indicate anomalies.

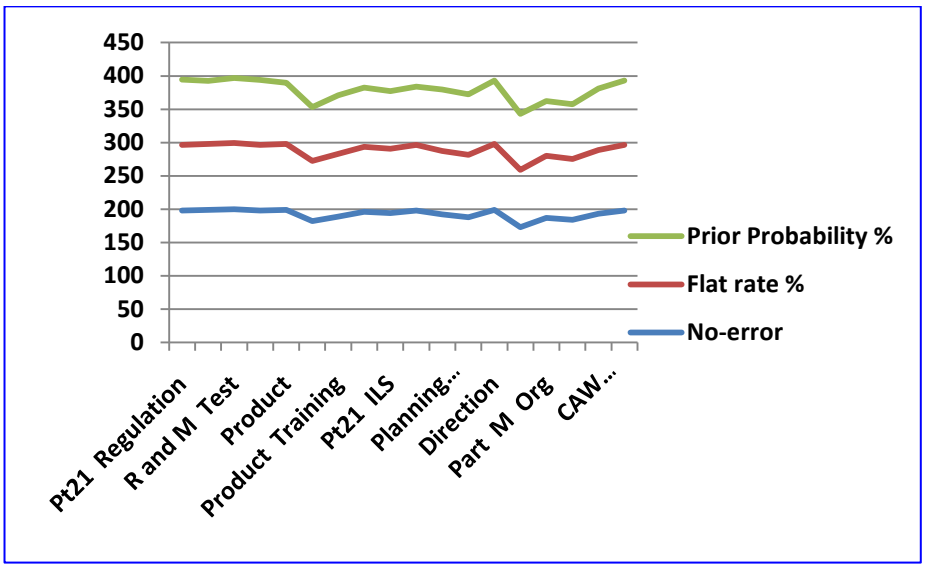


Figure 7.8 – Propagation of No-Error probabilities across the BBN

Similar tests were done on some of the other systems of the network with different configurations, and they were found to be behaving the same way. One other specimen result is given below for the Size of Operation Vs Capability subsystem, in which four separate groups of nodes feed into form a larger subsystem. For the tests,

501 CAW process cycles/flights were used. The behaviour patterns for the four individual groups are shown in Figures 7.9 to Figure 7.12, and for the combined group in Figure 7.13. Relevant data are in Table 7.3.

Node	Num of errors	Num of No-error	No error Flat rate %	No error Conditional Prior Probability %
Aircraft Group				
Aircraft_Type_Series_FW	0	501	100	96.7
Aircraft_Type_Series_RW	5	496	99.0	97.7
Registration_No	5	496	99.0	96.7
AC_Age	5	496	99.0	97.1
Sectors_Flown	5	496	99.0	97.1
Full_Maintenance_Cycles	5	496	99.0	97.1
Aircraft	5	496	99.0	91.6
Operation_Vs_Capability	5	496	99.0	90.7
Nature of Operation Group				
Ac_Generation_Time	5	496	99.0	98.4
Operational_Role	5	496	99.0	97.5
Route	5	496	99.0	98.2
Nature_of_Operation	5	496	99.0	96.9
Operation_Vs_Capability	5	496	99.0	90.7
Geographical Location Group				
Flight_Origin	5	496	99.0	96.5
Destination	5	496	99.0	96.5
Departure_Time	4	497	99.2	96.9
Geographic_Location_Time	5	496	99.0	94.9
Operation_Vs_Capability	5	496	99.0	90.7
Manpower Resources Group				
FleetSize_to_TR_Cat_A_Staff	3	498	99.4	98.8
FleetSize_to_TR_Cat_B1_Staff	3	498	99.4	98.8
FleetSize_to_TR_Cat_B2_Staff	3	498	99.4	98.8
FleetSize_to_TR_Cat_C_Staff	1	500	99.8	99.2
FleetSize_to_NonCat_Tech_Staff	2	499	99.6	99.0
FleetSize_to_Logs_Staff	3	498	99.4	98.8
FleetSize_to_Tech_Managers	2	499	99.6	99.0
Tech_Staff	5	496	99.0	97.2
Other_Support_Staff	4	497	99.2	98.5
Staff_Complement	5	496	99.0	96.9
Operation_Vs_Capability	5	496	99.0	90.7

Table 7.3 –Prior probability at nodes for No Error – Operation Vs Capability

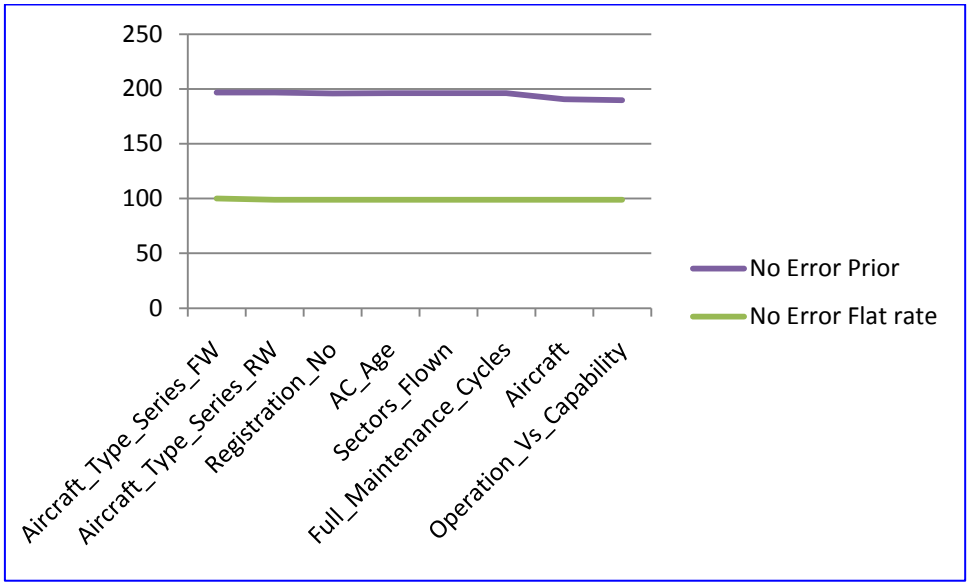


Figure 7.9 - Aircraft group - Propagation of No-Error probabilities

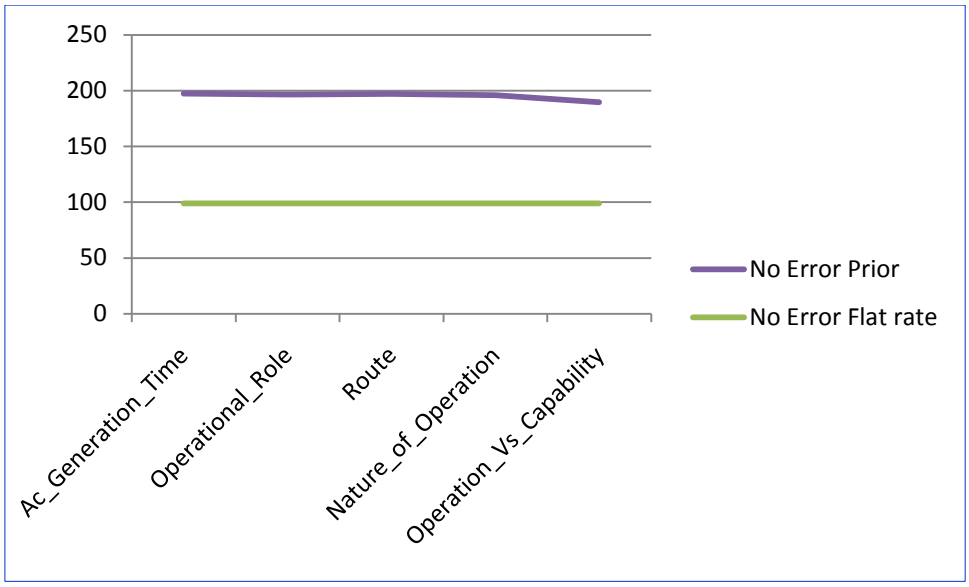


Figure 7.10 - Nature of Operation group -- Propagation of No-Error probabilities

Note that in the graphs for each of the individual groups, the right hand end terminating point is affected by interaction with the remaining 3-groups. The combined group, Figure 7.13, shows a certain amount of rippling effect in the area where the 4-individual groups begin to interact with one another. Even so, the deviations can be explained by observing the number of No-Error incidents, confirming that the underlying theoretical calculation of conditional probability was progressing smoothly.

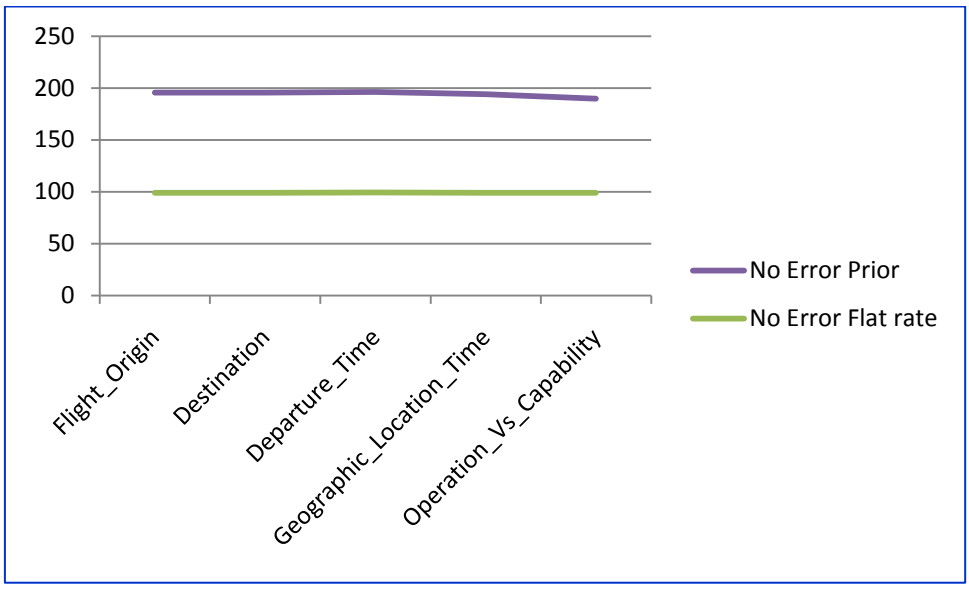


Figure 7.11 - Geographical location group - Propagation of No-Error probabilities

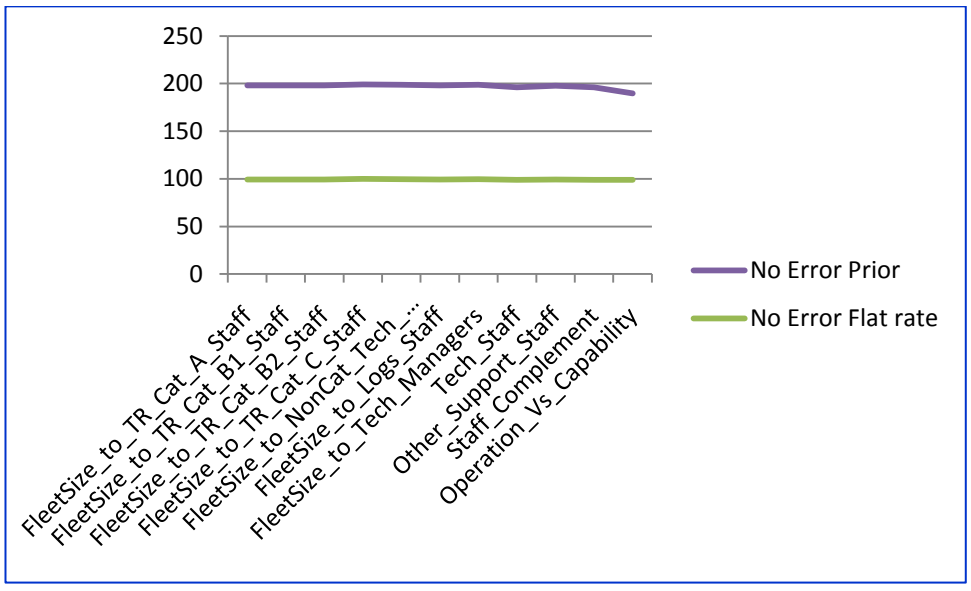


Figure 7.12 - Manpower resources group - Propagation of No-Error probabilities

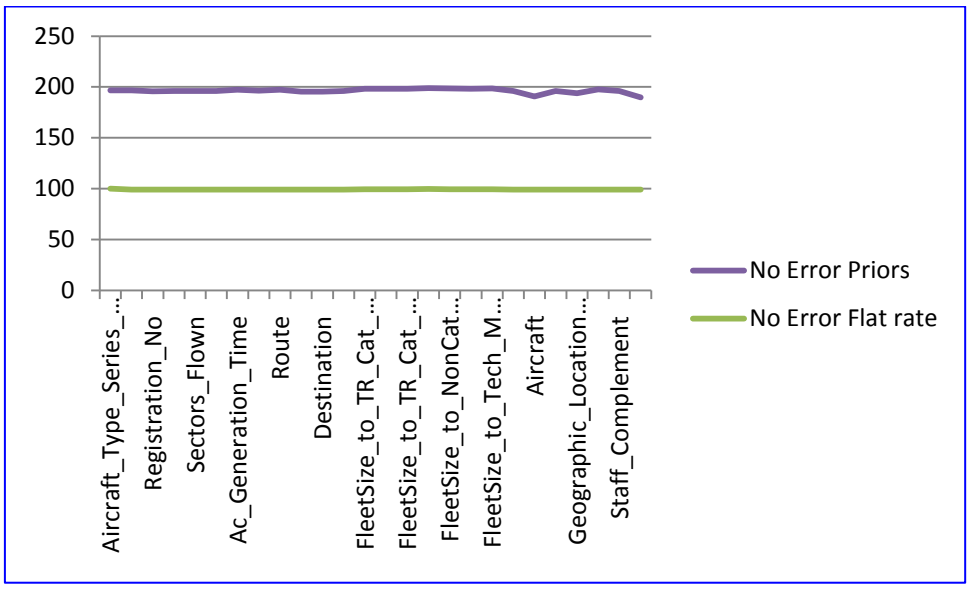


Figure 7.13 - Combined subsystem - Propagation of No-Error probabilities

The inference drawn from this observation is that the BBN computed results appear to be sensible. It is a rough check for gaining confidence that the computation software is doing its task properly, given that the proprietary software program algorithms and codes are not accessible to customers for their auditing.

Similarly, all other subsystems were checked out for accuracy, before the integrated model was run using a combination of data sets, 501 CAW process cycles/ flights. However, on this occasion, 2 non fatal (i.e. major) accidents were introduced into the dataset, as it is a simulation and more data was needed to see how the model behaves with data.

This data file is too large to be incorporated into the report as it cannot be reduced in size while retaining legibility. However it has been included in the attached CD, in Folder for Subsystem Tests.

Figures 7.14 to 7.20 demonstrate the tested status of each of the subsystems; Figure 7.21 (at the end of this chapter) presents the fully integrated model.

The results confirm that, given input conditions containing a high concentration of error incidents, the error probability at the exit end of each BBN is of the correct order as anticipated. This is of course not the scale of error probability that would be anticipated in a safe commercial environment. These results represent simulations to check if individual subsystems and the integrated model would work properly with data.

The belief bars, exposed, register the prior probabilities for the nodes concerned. The results indicate that each subsystem is returning sensible prior probability values for each relevant node consistently, and provides confidence on the integrity of the network architecture.

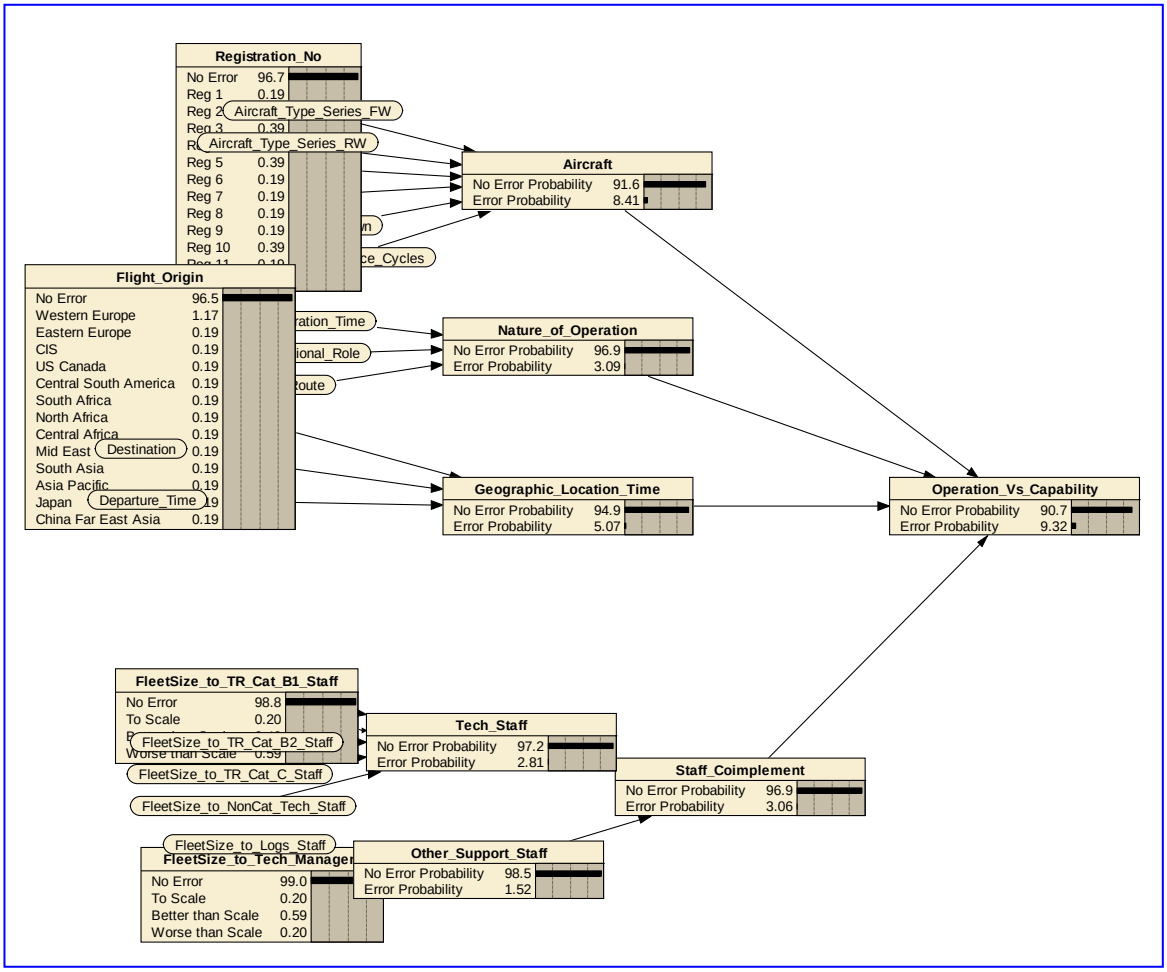


Figure 7.14 - Operation and Capability

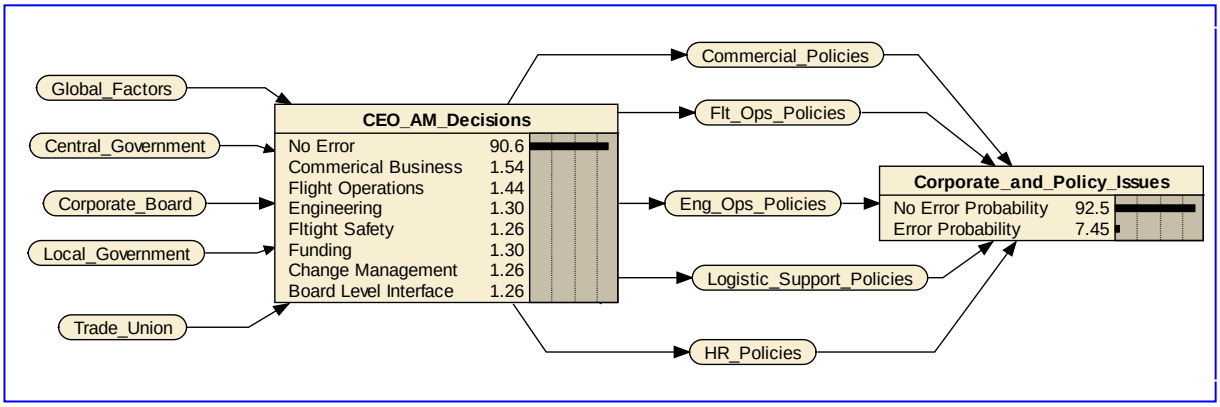


Figure 7.15 - Corporate Policy and Change Management

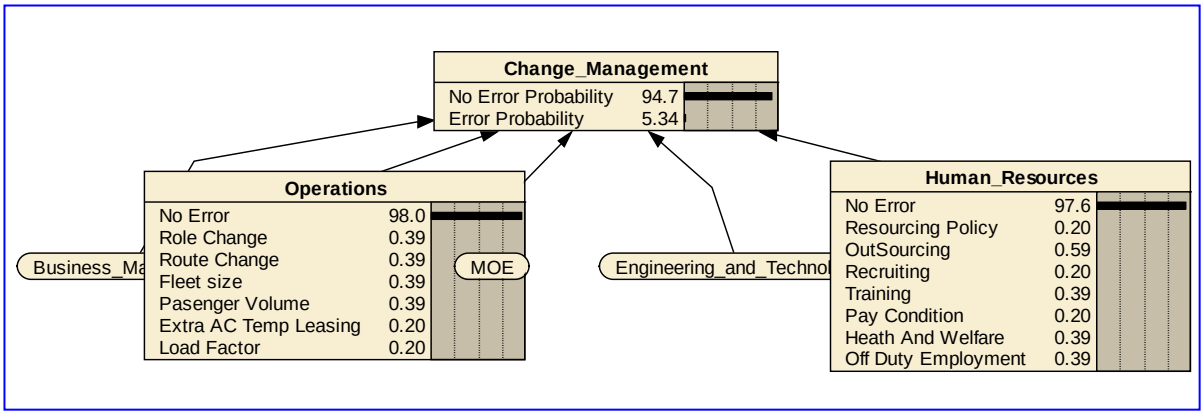


Figure 7.16 - Change Management

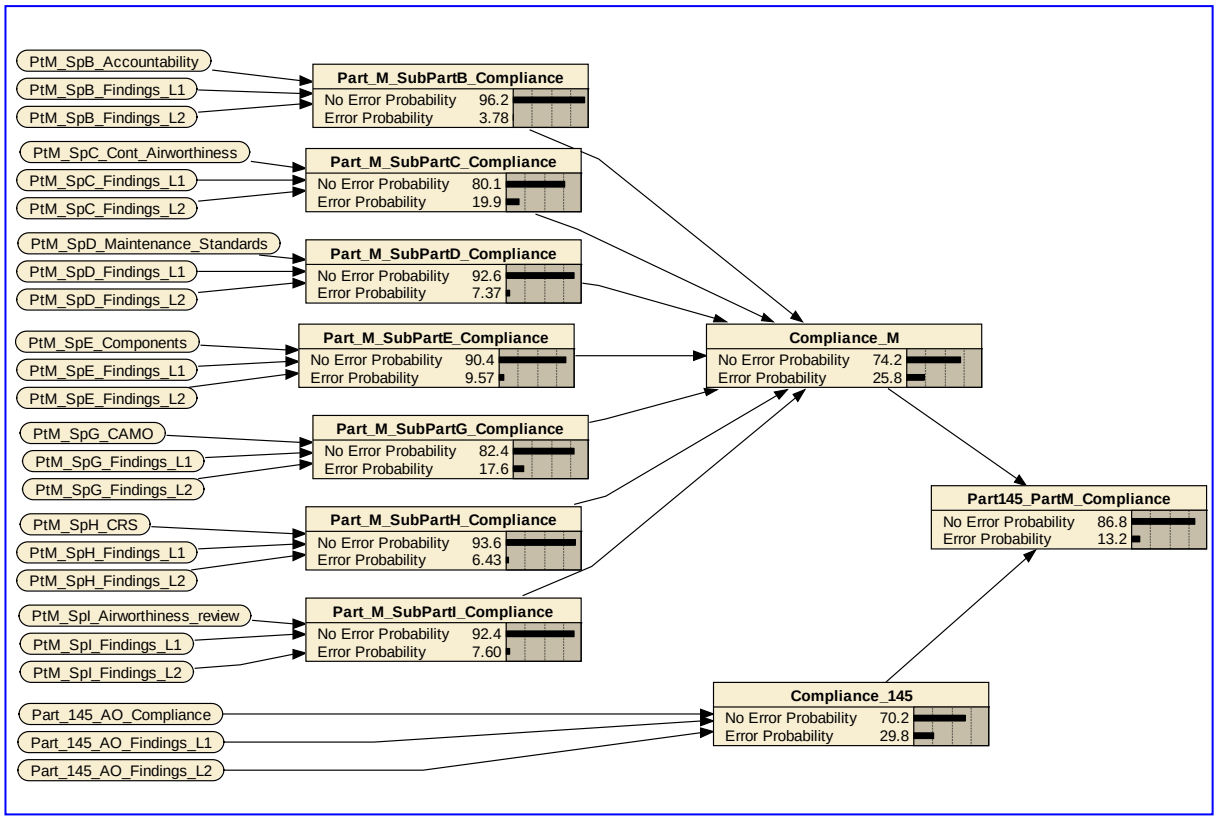


Figure 7.17 - Compliance Part M and Part 145 AO

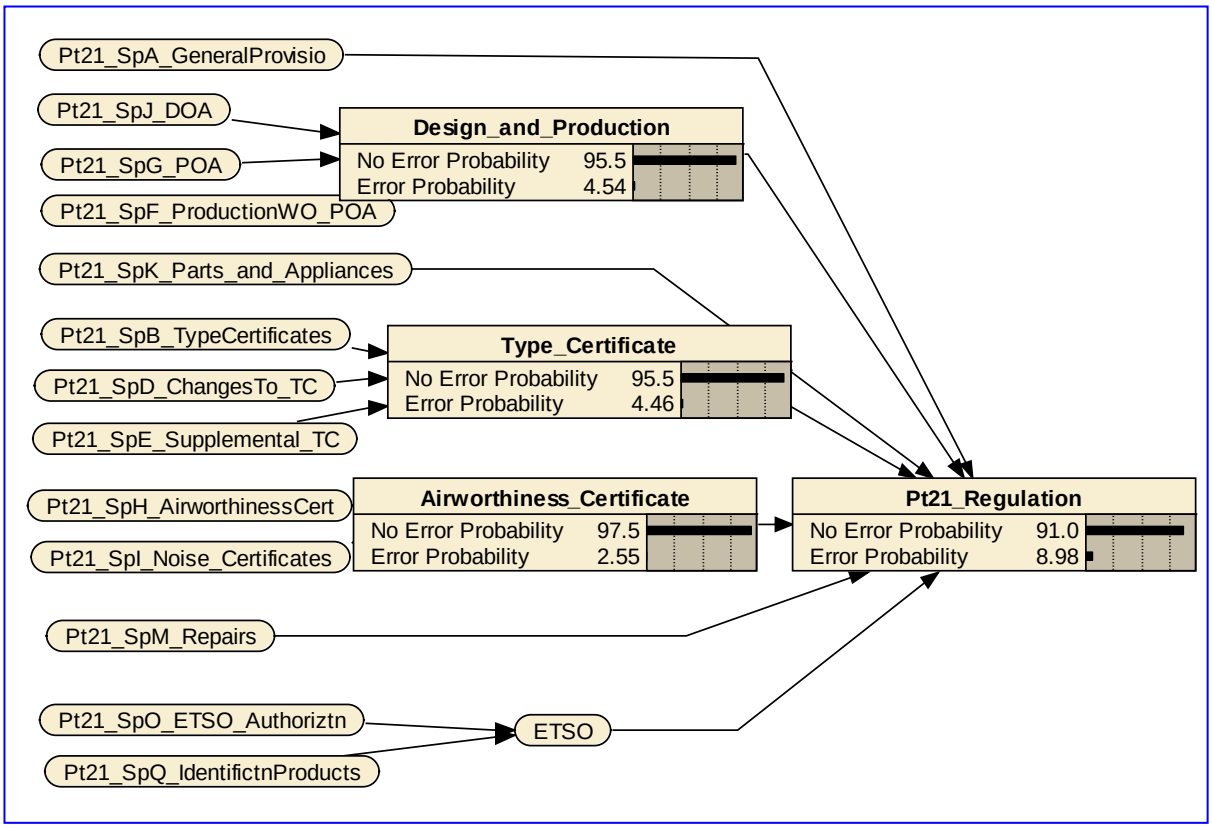


Figure 7.18 - Compliance Part 21 AO

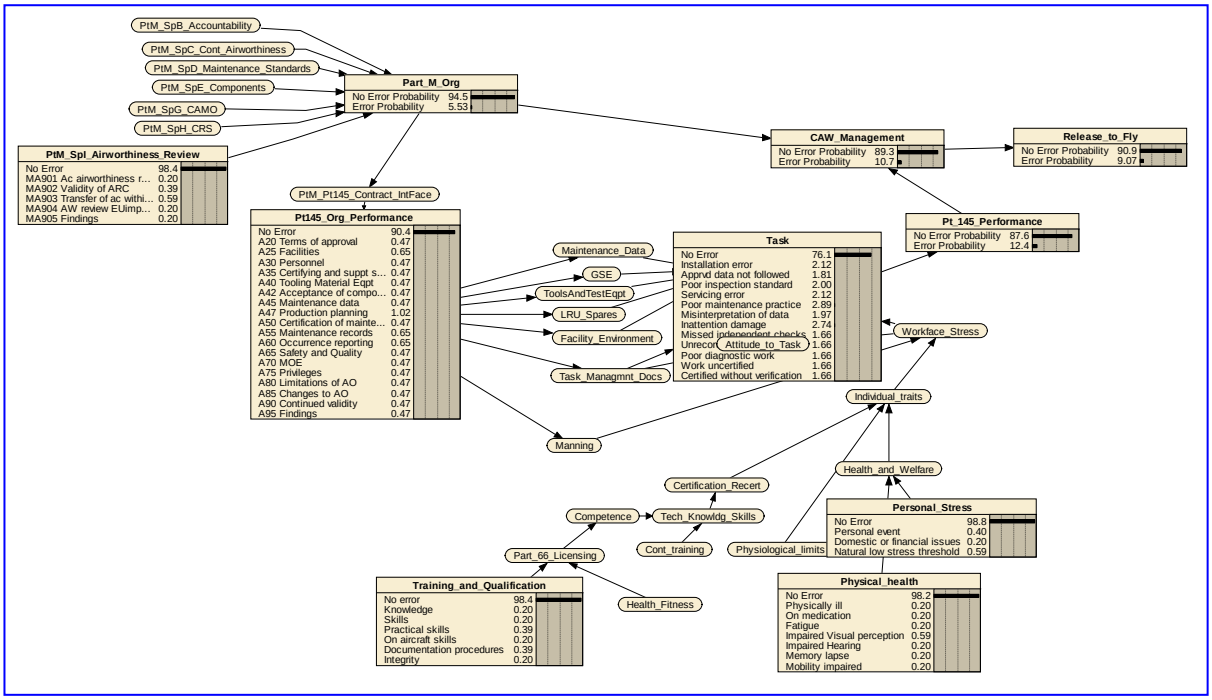


Figure 7.19 - Performance Jointly Part M, Part 145

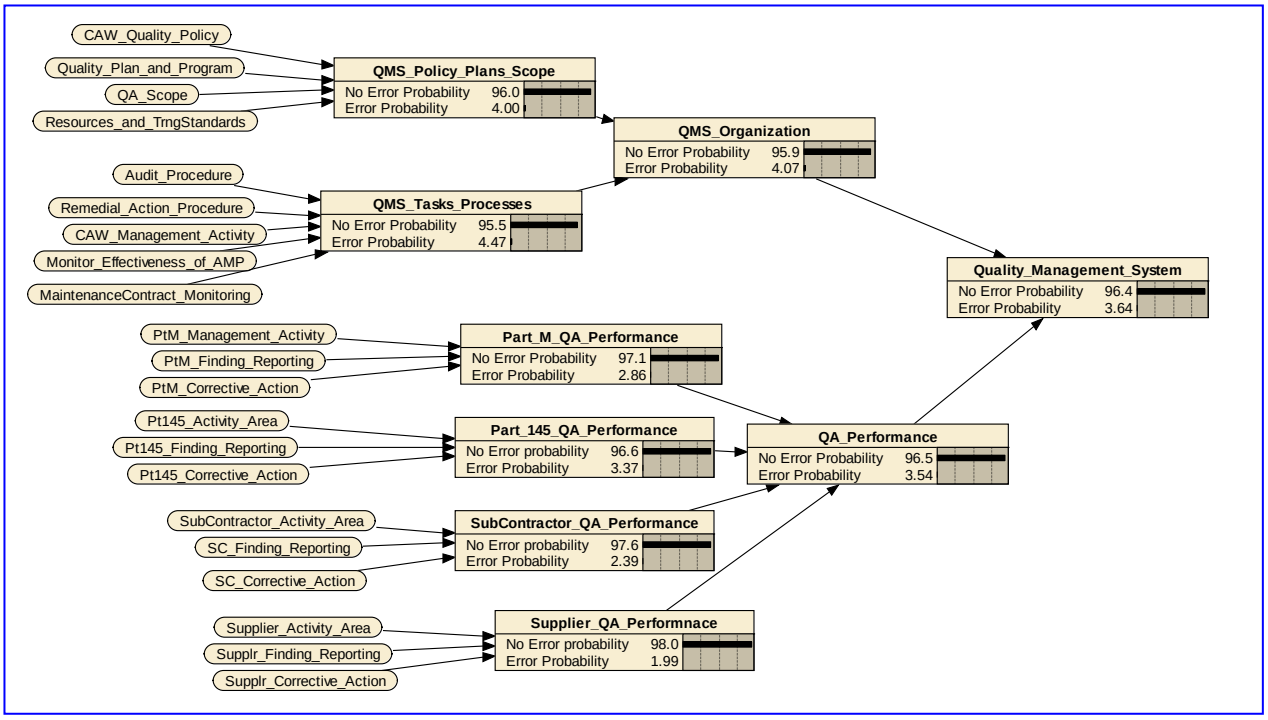


Figure 7.20 - Quality Management System

7.10 Overview - using the risk model

The integrated model, when uploaded and compiled, provides a snap shot of the dynamically stable state and the level of risk of that organization, which the error and no-error data represent. The state is represented by the prior probability of Error or No Error at each node. A dynamically stable system may already contain an unknown number of dormant errors and new error incidents, but the state is safe, as the effects of errors are considered to be either insignificant or are suppressed by design safety factors and defences built into the system. The system is dynamic because the CAW process, together with its participants, is continually in a state of transient. All organizations that safely conduct their civil aviation flight operations and engineering operations according to Regulation are expected to have dynamically stable systems. A significant flight or ground consequence would indicate that the dynamic stability has been compromised and tending to become unstable.

The model provides prior probabilities of error at nodal points of the CAW process on the basis of historic data up to that point in time. Each nodal point also provides the probability distribution of causal factors that contributed to errors. All this information could be either read off directly by examining the model, or be interrogated. In Figure 7.21 some of the nodes have been exposed in “Belief Bars” mode to illustrate the steady state prior probabilities.

Senior managers of an organization would be interested in the error probability at critical nodes, e.g. those representing Release to Fly, Handling & Despatch, and Takeoff. They might also focus on the probability of occurrence of various potential consequences of different levels of severity, conditional upon an initial dynamic stability of the system, and how they vary with errors elsewhere. Probability of error at each of these last 3-nodes is critical to the determination of risk at the output from CAW process, given all other error contributions and defences at upstream points.

As more new data are captured and processed, the model gets updated. Accordingly, the state should theoretically change but, in practice, in an organization that is dynamically stable and safe, the change might be hardly perceptible. However if changes become perceptible and significant, then it can be deduced that instability of the process is taking place somewhere within the system and this calls for an investigation to determine where the instability is taking place. In fact the model will show the sensitive spots which may be the roots of instability.

Sensitivity analysis, which will be described later in this section, helps to determine the nodes that might be likely sources of instability. This together with a node's probability distribution of causal factors will enable to pinpoint the source of instability, and to determine priorities for corrective actions.

The model can be used for drawing "what-if" type inferences according to posterior condition input nodes. This technique can be used for prediction purposes, i.e. for investigating the effect of any changes to an already dynamically balanced state of the organizations CAW process. This can be done by clicking the relevant causal factor at the chosen node, and by observing its effect at the end of the process, say, at Handling & Despatch node, or for that matter its effects on any other node in the model.

The same process could be followed to determine the effect of multiple findings, such as that would occur if a number of errors line up as that would occur in a system failure. In this case findings could be made at several nodes in a causal chain and the effect at the critical node could be observed. Naturally, if the output is not acceptable, i.e. exceeds a pre-determined threshold value, then urgent corrective actions should be taken.

Specimen readings from a primed model are given below and can be examined on the software files in the Folder for Integrated Model. Refer to CD File: *DJ CAW Risk Model_Combi 5_All_Ver2.*

7.11 Steady state

Table 7.4 and Table 7.5, which should be studied together, provide a specimen set of results corresponding to the steady state of an organization.

For demonstration purposes, only a few of the critical nodes of the CAW process have been selected; Table 7.4 Column (b) lists their prior probability of an error being "present" or "not present". These nodes represent critical milestones of the CAW process, i.e. at the Output of an aircraft from Pt 145 Organization, Completion of CAW Management by Pt M Organization, Releasing an Aircraft to Fly, Completion of Handling & Despatch and prior to Takeoff.

Given that CAW process is susceptible to human error, it is possible that some dormant errors from upstream activities of the process might have been carried forward to these nodal points. But these nodal points are defended, therefore some of the dormant errors might get detected and resolved, and others might be missed. Moreover, it is also possible that new human errors could get introduced due to manual intervention. Therefore the resultant error probability at the successive critical nodal points could fluctuate with experience, as recorded.

Status at key nodes	**Prior probability %**	**Posterior probability % (due to findings)**			
		Wrong funding decision	Dormant error in aged aircraft	Pt 145 LRU Spare - Faulty PMA part	Pt 145 Task – Poor maintenance practice
a	b	c	d	e	f
Part M Org					
No Error Probability	91.53	*86.9*	91.53	*66.8*	*84.3*
Error Probability	8.47	*13.1*	8.47	*33.2*	*15.7*
Pt 145 Performance					
No Error Probability	82.8	*71.9*	82.8	*51.6*	***37.5***
Error Probability	17.2	*28.1*	17.2	*48.4*	***62.5***
CAW Management					
No Error Probability	88.2	*82.5*	88.2	*71.0*	*66.0*
Error Probability	11.8	*17.5*	11.8	*29.0*	*34.0*
Release to Fly					
No Error Probability	90.4	*86.7*	90.4	*79.2*	*76.0*
Error Probability	9.61	*13.3*	9.61	*20.8*	*24.0*
Handling Dispatch					
No Error Probability	87.4	*82.5*	*79.8*	*81.8*	*81.1*
Error Probability	12.6	*17.5*	*20.2*	*18.2*	*18.9*
Take Off					
No Error Probability	92.6	*90.2*	*88.8*	*89.8*	*89.5*
Error Probability	7.45	*9.81*	*11.2*	*10.2*	*10.5*

Table 7.4 - Probability of Error at Key Nodes *(Italics indicate change)*

Usually, practical CAW process activities on an aircraft terminate at the end of "Handling & Despatch" event, unless the aircraft had to return to the gate or the aircraft captain called for any running repairs. Therefore "Handling & Despatch" is an appropriate point where the final probability of error attributed to CAW could be assessed.

Once an aircraft is despatched and before takeoff, the flight crew could discover a previously undetected CAW. In this case the aircraft might either return to the gate for disembarking passengers, or if not it might undergo a running repair while passengers remain on board; however if the flight crew decided that the error was not serious enough to delay the takeoff then the flight might continue without interruption.

Alternatively, if there was a dormant error and yet, if it was not detected at takeoff, then the error would be carried forward. The flight might either continue safely to its destination or, if not, experience a flight incident with further consequences.

Status at key nodes	Prior probability %	Risk = Error Probability x Consequence	Posterior probability % and Risk			
			Wrong funding decision	Delta Risk	Error related to an aged aircraft	Delta risk
(a)	(b)	(c)	(d)	(e)	(f)	(g)
Flight and Consequences						
No Error	92.1		*89.9*		*88.7*	
Flt Completed Error CF No Cost	0.80		*1.0*		*1.11*	
In Flt Shutdown Flt Completed	1.43		*1.82*		*2.04*	
Incidence RTB	1.43		*1.82*		*2.04*	
Incidence Flt Diverted	1.43		*1.82*		*2.04*	
Non Fatal Accident	2.05		*2.63*	*+0.58*	*2.97*	*+0.92*
Fatal Accident	0.80		*1.0*	*+0.20*	*1.11*	*+0.31*
Combined Cost (Including cost of detected errors)						
No Cost	84.7	0	*82.9*		*81.9*	
Cost group 1 > £10	1.54	1.5p	*1.71*		*1.80*	
Cost group 2 > £100	1.67	£1.67	*1.84*		*1.93*	
Cost group 3 > £1,000	1.68	£16.80	*1.84*		*1.93*	
Cost group 4 > £10K	1.56	£156	*1.76*		*1.87*	
Cost group 5 > £100K	1.61	£1610	*1.84*		*1.97*	
Cost group 6 > £1M	1.64	£16.4K	*1.90*		*2.04*	
Cost group 7 > £10M	1.39	£139K	*1.56*		*1.65*	
Cost group 8 > £100M	1.39	£1.39M	*1.56*		*1.65*	
Cost group 9 > £1B	1.39	£13.9M	*1.56*	*+£1.7M*	*1.65*	*+£2.6M*
Cost group 10 > £10B	1.39	£139M	*1.56*	*+£17M*	*1.65*	*+£26M*

Table 7.5 - Consequences and Risk *(Italics indicate change)*

Table 7.5, under “Flight and Consequence”, lists consequential effects of errors carried forward in a flight, as well as those detected during the CAW process and prior to take off.

There could be a range of different consequences, which, according to past experience, could be represented as different prior probability densities, Column (b). Associated with in-flight consequences and detected errors prior to take off is a cost element. All these cost elements have been pulled together under Combined Cost. In this simulated exercise they were test estimates (arbitrary figures) that fell within cost bands rather than actual costs.

If both the probability of consequence and its numeric value (in this case the cost) are known, then the risk could be determined as a single figure. But as explained in Chapter Two and Chapter Three, risk is conditional. Experience would show that conditions prevailing in an organization could produce any one of several possible outcomes at different occasions, and Consequence nodes reflect the full range of possibilities and their probability density distribution.

The output “Combined Costs” is a good representation of the overall cost of error, irrespective of the fact that errors end up either as incidents or are detected in the process and managed.

These outputs jointly provide full information on the risk level of that organization based on its performance, which may be more meaningful and of interest to AM/CEO than a single number risk level.

A manager familiar with the model could choose any one of these nodes from the model, to examine its status in order to gain an insight to the overall performance of the organization. The error probability data at different significant process stages of the organization, consequences as well as range of probability values of cost of consequence can be made available. Some of the nodal points of the process are both safety and business critical to the operation. These are “Release to Fly, “Handling & Despatch” and “Takeoff” points. The more upstream nodal points are indicative of primary root causes and dependent error sources where corrective actions and funding priorities might be needed.

Should an AM/CEO call for a single number risk level for the organization as a Key Performance Indicator (KPI), e.g. the maximum risk or an average, the highest risk and mean of the probability range could be obtained.

7.12 Prediction

Given a prior condition, it is possible to use the model to make predictions, for example to determine the effect of a potential new error in any of the input nodes, which is referred to as a "Finding". "Finding" is either a detection of an error, a consequence, or a change of condition to a dynamically stable process system, such as an error of judgment in decision making. A decision relating to either a reduction of funding, manpower resources, or a hasty engineering operation forced on by time-pressure and commercial consideration is a case in point.

By simply selecting the relevant node and causal factor the model will compute the effect of the conditional change of state on the error probabilities at critical nodes of interest and their potential consequences. Thus the risk level information is available to the organization and its managers. This new state is called "Posterior Probability".

Table 7.4 Columns (c) to (f) and Table 7.5 Columns (d) and (f) demonstrate the way probabilities at critical nodes change in response to change of conditions at upstream nodes, in these examples a single change of conditions has occurred. Similarly multiple errors or a simulated causal chain could be induced to determine the error probability at critical points, potential consequences and hence risk.

Whether or not the states predicted are acceptable or not is a matter for the AM/CEO of the organization and the national authority. This thesis will discuss that issue in Chapter Nine. It is reasonable to state that there should be an agreed benchmark. Though it might be difficult to negotiate a benchmark, it is technically possible. This model provides a management tool that enables the setting up of such benchmark for the individual organization and possibly for the industry.

7.13 Dynamic state

Steady state snapshot and capability to predict is not the end of the story for this model. Conditions of the organization change with time, and therefore the risk level. The complete interactive CAW process is in a dynamic state and therefore the database must be kept updated continually in order to gain information on the organizations risk level.

Thus, the model recognizes the fact that the risk level of an organization could fluctuate from moment to moment, but from a management viewpoint the objective is to maintain the risk level below an accepted threshold, or better still, to gradually

reduce it, ideally to zero risk. The model provides this capability to monitor and manage the risk level almost in real time, and therefore the risk assessment can be an on-going live process based on a systematic rationale rather than on a periodic review, if any, that usually precedes an oversight inspection.

7.14 Sensitivity test

Sensitivity tests can determine how sensitive the risk level is to input parameters. In this case input parameters are the errors that occur in the CAW process, in compliance with regulation as well as shortfalls in defences such as quality audits. The tests pinpoint which nodes (i.e. events and causal factors) have an impact on critical nodes of interest, and what their order of importance is. Sensitivity of any identified node/ parameter to changes in another node/ parameter can be tested by making a "Finding" at the input node (i.e. the independent) and then by observing the response of the critical node of interest (i.e. the dependent).

Having identified the dependent and independent nodes to be examined, the test starts with the steady state. With a finding made at each parameter of the independent node, the maximum and minimum values of the response at the dependent node can be observed.

The exercise can be repeated for each one of the remaining independent nodes in turn, observing the response at the dependent node. By examining the range of responses, and amplitudes, it is possible to determine which of the independent nodes have the greatest response at the dependent node. Based on these results, the independent nodes can be ranked in the order of their importance.

Sensitivity test on the nodes of a complex network can be extremely tedious if it were to be undertaken manually, node by node. Therefore, NETICA software has been designed to perform this function such that it can test all the nodes and their states of nature rapidly. All nodes could be sensitivity tested to determine which ones are significant or critical to the CAW process or the CAW management or business function.

The software reduces the results and presents them as a metric called "Reduction of Entropy" which is a measure of sensitivity. Larger the entropy reduction assigned to a node, greater is the sensitivity. Advanced statistical theories relating to sensitivity tests used in NETICA are described by Spiegelhalter (1989)[89] and Neapolitan (1990)

page 394[100], whilst the theory relating to Reduction in Entropy has been explained by Pearl (1988) page 321[101].

The practical procedure for undertaking a sensitivity test with NETICA program is explained in the NETICA User Guide. A small part of a sensitivity test output is reproduced below for demonstration purposes, Table 7.6.

Probability ranges	Min	Current	Max	RMS Change
No error	0.08333	0.9207	0.9881	0.2375
Safe flight-error carried forward	0.001988	0.008046	0.08333	0.02136
In flight shut down	0.001988	0.01425	0.1667	0.04324
Incident returned to base	0.001988	0.01425	0.1667	0.04324
Incident – Flight diverted	0.001988	0.01425	0.1667	0.04324
Non fatal accident	0.001988	0.02046	0.25	0.06511
Fatal accident	0.001988	0.008046	0.08333	0.02136

Entropy reduction = 0.2836 (47.4 % 0f 0.59873 max given in Table 7.7)

Table 7.6 - Sensitivity of 'Flight and Consequences' to findings at 'Takeoff'

In this example, the selected independent node is “Flight and Consequences”. The output is based on 501 simulated CAW process cycles/ flights used for testing the model. The test checks the sensitivity of “Flight and Consequences” node to Error and No Error inputs from the preceding node “Takeoff”.

Current values are the prior probabilities following uploading data and compiling. Min or Max values are the probabilities taken by each of the parameters (states of nature of Flight and Consequences node) when Takeoff node’s state of nature has either the minimum probability value or the maximum probability value respectively.
For instance, “Takeoff/No Error” takes a min value, if a finding is made in “Takeoff/Error”. This would give a corresponding min value in “Flight & Consequences” at “No Error”, and gives max value in “Flight & Consequences/Other States of Nature”. Similarly, “Takeoff/ No Error” takes a max value when it is 100%. If there is certainty that all flights at “Takeoff” are free from error, this could be indicated by making a finding and that would give a maximum value to “Flight & Consequences/No Error”, and minimum values to the remaining states of nature of that node.

RMS is the root mean square, which is the square root of the average of the values squared; it gives information on how each state of nature in the query node (i.e. “Flight & Consequence”) behaves in response to changes in variable node (i.e. “Takeoff”). The larger the value of RMS change the greater the sensitivity. In this case, “No Error” state is the most sensitive to change in “Takeoff” conditions, with

sensitivity decreasing in non-fatal accident, followed by the group of 3 consequences ("In-flight shutdown", "Return to base" or "Flight diverted" and the least sensitive final group("Error carried forward" and "Fatal accidents"). Careful observation of the error pattern and common sense judgment would probably have given the same answer but in retrospect, quantitative data from the analytical process provides a higher level of confidence than that is attributable to expert judgment.

This form of analysis could be repeated for each of the nodes in the model.

NETICA uses the "entropy change" to measure of sensitivity of the entire node. Entropy change could be visualized as its level of instability or readiness to change, hence its sensitivity.

Entropy reduction (designated I) has been defined as the mutual information between the query variable (in this case "Flight and Consequences" designated as Q) and the varying variable (in this case "Takeoff" designated as F) measured in bits.

Norsys Software Corporation, in a private correspondence, has provided this study with the underpinning mathematical analysis as follows:

Reduction of entropy I = H(Q) – H(Q|F), where H(Q) is the entropy function for query node: This is the summation of $P(q)\log_2 P(q)$ for each state of Q, from 1 to n.

$$H(Q) = \sum_{q=1}^{n} P(q).\log P(q) \quad \text{..... 7.1}$$

H (Q|F) is the entropy function for query node, given probability of variable occurring. This is the summation of $P(q|f)\log_2 P(q|f)$ for each state of Q, from 1 to n and for each state of F, from 1 to n.

$$H(Q|F) = \sum_{q=1}^{n} \sum_{f=1}^{n} P(q|f).\log P(q|f) \quad \text{..... 7.2}$$

$$I = \sum_{q=1}^{n} \sum_{f=1}^{n} P(q|f).\log P(q|f)\,/P(q).P(f) \quad \text{..... 7.3}$$

NETICA program undertakes this complex calculation and outputs the result as an Entropy Reduction for the query node related to the variable node. Unless the variable nodes were specified prior to the sensitivity test, NETICA outputs Entropy reduction associated with all the nodes in a descending order. Transcribed below are the first 20 variable nodes and the entropy reductions associated with the query node Flight & Consequences, Table 7.7.

Node	Mutual Info
Flight and Consequences	0.59873
Take Off	0.28358
Combined Cost	0.19423
Handling and Dispatch	0.13358
Release to Fly 1	0.02057
Operation Vs Capability	0.01971
Defence Pre TO	0.01794
CAW Management 2	0.01165
Quality Management System	0.00777
Consequence Pre-TO	0.00738
Defence Handling and Dispatch	0.00658
Pt 145 Performance	0.00424
Aircraft	0.00410
Geographical Location and Time	0.00236
Consequence Handling and Dispatch	0.00234
Defence Pt M	0.00174
Nature of Operation	0.00140
Staff Complement	0.00139
Attitude to Task	0.00132
Pt145 Org Performance	0.00124

Table 7.7 - Specimen output from sensitivity analysis

Taking this concept forward, Table 7.8 lists the relative sensitivity of output at a number of query nodes in response to various input parameters, e.g. “Combined Cost”, ”Takeoff” and “Handling and dispatch”. In each situation the top-ten nodes that have the most significant impact on the selected query node are listed in descending order.

7.15 Significance of sensitivity test

Sensitivity tests are significant for the direction and control of a process system through identifying and monitoring Key Performance Indicators (KPI). The test helps to determine which of the nodes are important, and which other nodes have the greatest impact on them. In a very complex organization, it is not possible for the higher management to monitor all aspects of the process, and then they should resort to identifying one or few nodal points of importance. This capability is of interest to the AM/CEO in order to identify those KPI that AM/CEO or his deputy ought to monitor for the welfare of his organization that depends on the integrity of end product, this being flight safety.

Rank	Combined Cost		Take Off		Handling and Dispatch	
	Finding at Node	Entropy Reduction = Sensitivity	Finding at Node	Entropy Reduction = Sensitivity	Finding at Node	Entropy Reduction = Sensitivity
(a)	(b)	(c)	(d)	(e)	(f)	(g)
1	Flight & Consequences	0.194	Flight & Consequences	0.284	Take Off	0.169
2	Take Off	0.150	H & D	0.169	Flight and Consequences	0.134
3	H & D	0.078	Combined Cost	0.151	Combined Cost	0.078
4	Consequence of Detected Error at H & D	0.051	Release to Fly	0.026	Release to Fly	0.067
5	Consequence of Detected Error at Release to Fly	0.048	Operation V Capability	0.025	Operation V Capability	0.065
6	Consequence of Detected Error at Release to Pt M	0.046	Defence Pre TO	0.022	CAW management	0.025
7	Consequence of Detected Error at H & D	0.043	CAW Management	0.015	Defence H & D	0.022
8	Consequence of Detected Error at Pre Take Off	0.032	QMS	0.010	Pt 145 Performance	0.014
9	Consequence of Detected Error at Pt M Org	0.030	Consequence of Detected Error at Pre Take Off	0.009	Aircraft related errors	0.013
10	Consequence of Detected Error at Pt 145 Org	0.025	Defence H & D	0.008	Task related errors	0.009

Table 7.8 - Sensitivity test results

Deep within the process are other nodes where often those errors at the bottom of "the error iceberg" reside. Local managers who are responsible for these process subsets could check the sensitivity of their output to related inputs, quite often affected by policy decisions. Management reports that are supported by factual numeric data rather than speculation and guesswork should improve communication with AM/CEO.

It should be stated here that performance indicators for organizations derived through sensitivity tests could be different from one organization to another. This is because every organization has a unique behavioural pattern that generates different error

probabilities and consequences in addition to the variation of natural conditions that lead to incidences. Traditionally the uniqueness has been termed the “culture” of the organization either for a lack of suitable terminology to describe its individual signature. Whilst this study refrains from generating another terminology to replace “culture”, through the model, it provides a rationale to explain why such differences exist.

Human behaviour and variability of conditions are such, one cannot expect uniformity between organizations. Human errors occur despite regulation and standards. It is not always possible to achieve an error free ideal, because human behaviour and error occurrence do not follow or cannot be controlled by dictate. One possible way forward for improvement is to give organizations the right tools to prove that whatever their culture, they could monitor their performance, gradually improving their own signature and eventually turnout an error free, safe aircraft consistently. This study provides an insight to this truth.

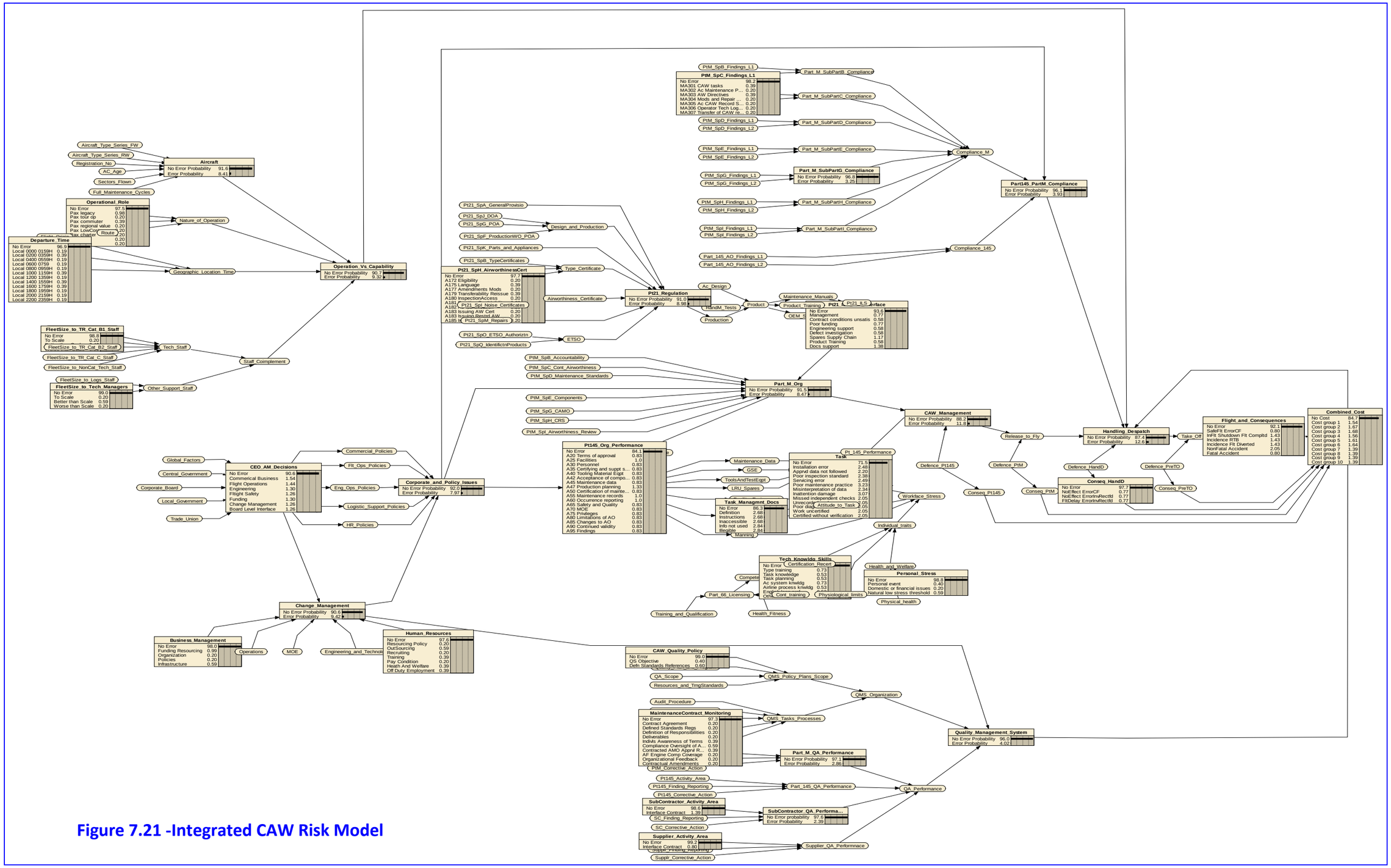


Figure 7.21 -Integrated CAW Risk Model

Intentionally Blank

Chapter Eight
Model validation using field data

8.1 Validation trial

The CAW Risk Model was validated using field data from a commercial, civil aviation operator, designated as Operator X. The aim of the validation trial was to investigate if the model has value as a practical risk assessment tool in industry, whereas its short term objective was to ascertain if the model could be used with currently available field data, and if the results were meaningful and sensible. Presenting the outcome of the trial in the closing phase of the research study, this chapter describes the challenges that had to be overcome and how they were addressed.

8.2 Preamble on Model

To recap on the previous work, the generic CAW Risk Model used for validation is a maintenance-centred Bayesian Belief Network, which represents factors that influence the continuing airworthiness process of a commercial aircraft. The model at this point contained 175 nodes and 1,094 parameters. The nodes represent various elements of the CAW process, where errors, defences or consequences of error occur. In order to provide maximum coverage of process events and causal factors of error, as many of them as practically possible have been taken into account, whilst acknowledging that there might be some unforeseen gaps in the coverage. If so, then the model should provide a way of dealing with the unknowns. This issue will be addressed later.

At each node, its states of nature define if an error is present or not according to the taxonomy of causal factors designed for this model. Some nodes record management information, such as type and registration number of aircraft or the maintenance station where the error had occurred.

The model has been designed to capture information about the CAW process that takes place between consecutive flights as well as the consequences, i.e. if the CAW process was error free or erroneous, if the error was detected and defended or if missed then what the flight or ground consequence was. Data capturing is repeated sector by sector consecutively.

Despite the models capability to capture a wide range of data, only few nodes will be actually needed at any one time to record information relevant to an error

occurrence. All other nodes would simply record “No Error” status, because they have neither contributed nor indirectly related to the error occurrence. If the CAW process between two consecutive sectors flown did not show up any errors, then all nodes would register “No Error” information.

Errors captured by the model fall into 3 categories according to the way they were discovered and reported.

- Reactive errors, revealed as a result of an investigation into a ground or flight incident to an aircraft, equipment or to personnel.

- Pro-active errors, which are either recognized as they occurred or discovered by personnel in the course of their normal work. Some of these errors might have occurred on an unknown date and time, and could have remained dormant until their discovery.

- Errors detected as a result of an oversight inspection or a routine local quality audit. These were grouped under pro-active category for the validation trial.

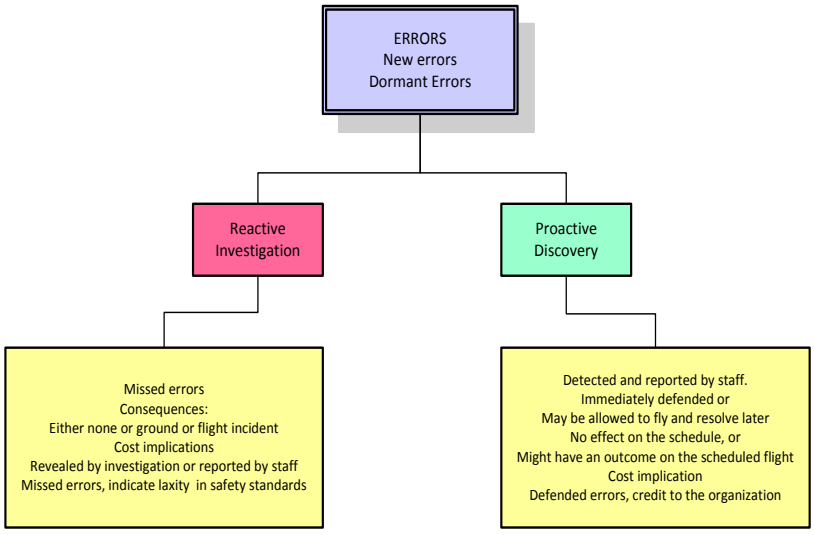


Figure 8.1 – Error incidents according to how detected

All errors, if detected, are expected to be defended. Obviously, those errors detected before an aircraft is released to fly would improve flight safety, which is a credit to the organization. Depending on their potential consequences, some detected errors might be documented and be authorized to be carried forward as deferred defects until a suitable opportunity was found to correct them provided that they do not undermine flight safety.

Conversely, missed errors underscore the fact that the organization should improve upon safety standards. Errors, detected as a result of investigation, might have already had a detrimental consequence, but defending them even retrospectively would be important to prevent recurrence, and to promote flight safety.

All errors, missed or detected, would have an eventual cost implication. Missed errors that are either detected after "release to fly" or lead to incidences during the flight phase could have a significant cost impact. A timely detected and defended error might be dealt with lightly, so far as the affected flight is concerned.

Provision has been made in the model's design to collect cost data, despite that the industry does not appear to be interested in collecting cost data related to human error. Several organizations informed this study that they did not maintain specific cost data related to maintenance human error. Generally costs are absorbed into the standing maintenance cost overhead on the belief that separate accounting may be uneconomical.

8.3 Field data source requirement

According to the research objectives, the model was to be used to determine risk in continuing airworthiness attributed to human-error. Whatever the hazards attributed to human error that comes from one approved organization, their contribution to risk can be assessed by the model. It then becomes a measure of reliability of the organization own performance. Concurrently, the model identifies contributions from other external influences, organizations and processes that might have generated the root causes of the error. Data flow must be continuous and causal chains identify both internal and external error sources.

The model can be utilized by one approved organization such as an MRO that provides Base servicing support to a number of aircraft operators, as in Figure 8.2. All data that is taken into account for risk calculation must come from that one named organization, and those related to it where causal chains extend to others, such as Part 21 POA or DOA. However, the risk calculation for the organization should be based only on those errors attributed to the approved organization and its staff. If not it would be unfair to the organization. All error occurrences and consequences ought to be captured and it should be possible to authenticate the event and details through documentary evidence to safeguard the reliability of data.

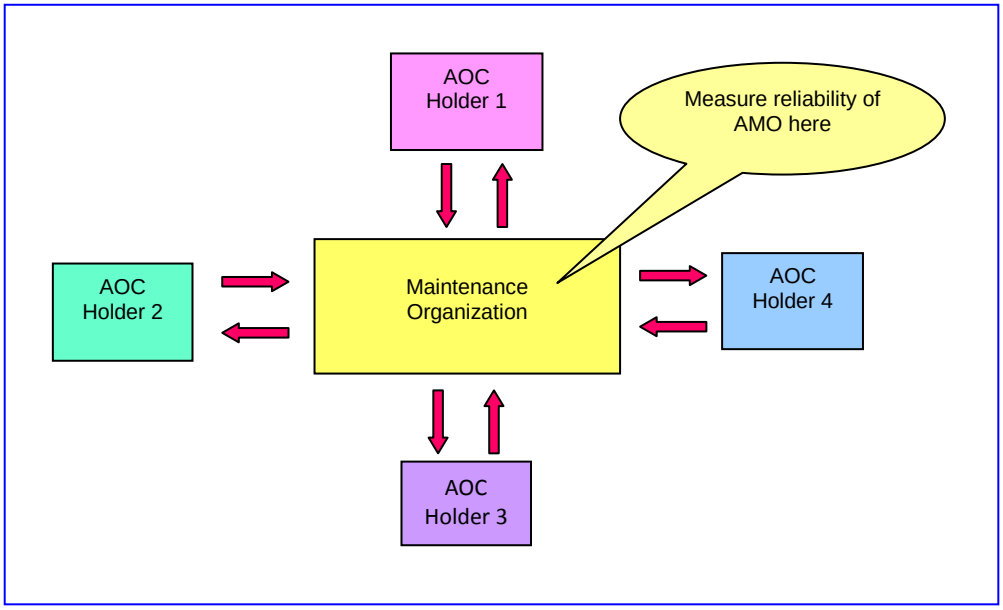


Figure 8.2 – Synergy between maintenance organization and operators

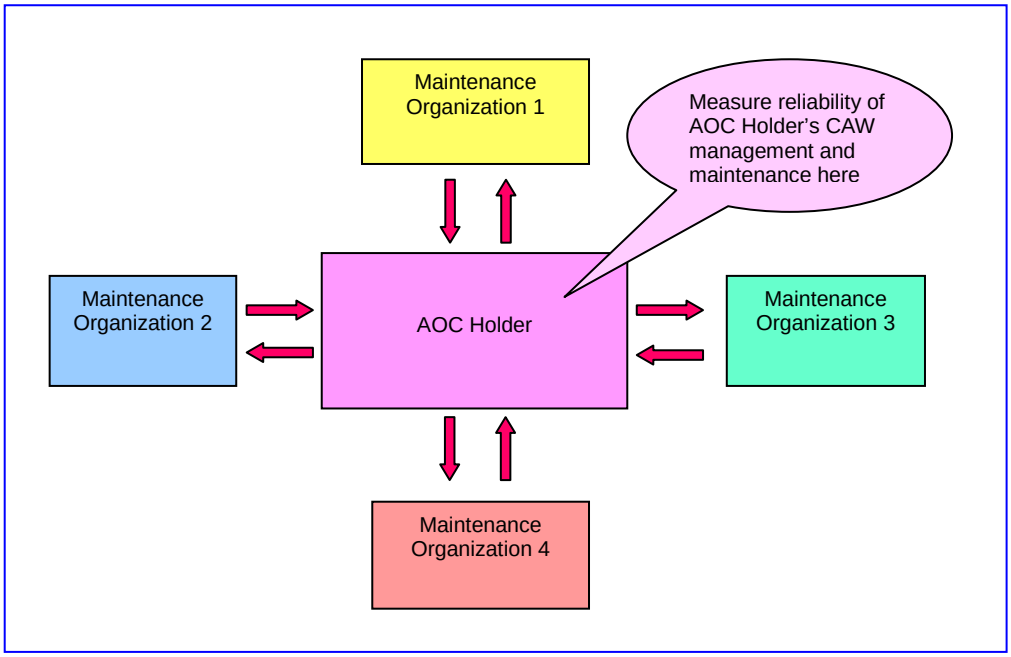


Figure 8.3 – Synergy between operator and maintenance organization

Where an AOC Holder undertakes flying operations that involve more than one approved organization, as in Figure 8.3, the model can be used to measure the reliability of the overall operation instead of one approved organization providing maintenance support. In this arrangement, the model can be used to determine the risk to continuing airworthiness from a complex network of maintenance organizations, whose operation is coordinated by one AOC Holder. This is in fact the reality for most fleet operations that contains a large amount of route flying within a

pre-planned network. In this situation, the focus of attention is the AOC Holder and his fleet and the risk is measured against the named fleet. Therefore, all the input data must be related to that named fleet, regardless of the fact where or in which maintenance organization the CAW errors occurred or discovered.

8.4 Exclusion of public domain databases

Data from public domain accident investigation databases such as UK AAIB, NTSB, Canadian Transport Safety Board, have been excluded from validation trial as unsuitable data. This type of database did not maintain all relevant data for the whole fleet or a particular organization, year on year. Any useful data for this study must be linked to a specific maintenance organization or fleet, and they must be continuous, complete and accountable.

8.5 Potential data source options

Given these conditions, the study faced one of its main challenges, that was, "how to obtain authentic error incidence data from operators and maintenance organizations". Through background research, it was known that approved organizations were required by regulations to maintain a register of maintenance error occurrences as part of their Maintenance Error Management System (MEMS), UK CAA CAP 562 Leaflet 11-50[51]. All error occurrences, regardless of their severity of consequences, are recorded here, even though only a few of them might be investigated subject to the discretion of organization's management. Nevertheless, MEMS database was considered more likely to provide the study with a fully documented and reliable record of error occurrences, as well as detailed investigation reports where possible. This database, together with information on error-free sectors flown and other aircraft utilization data would give the study a capability to calculate error probabilities.

Key items in the required data list were details of maintenance errors encountered, findings of quality audits and compliance oversight inspections, together with their supporting information. Information regarding the operator's organizational structure, its general procedures relating to engineering operations, types of aircraft, roles, and staff complement were examples of supporting data. Appendix 9 lists the full details of data items that were desired and or requested.

8.6 Potential participants

Identification of the type of data needed was only part of the challenge. The other part was the identification of operators that was willing to participate in the validation trial by supplying relevant data. This is because MEMS data were considered as proprietary data by their owners, and UK CAA had agreed to this status. As such, general public had no right of access, particularly when the owners considered that they are commercially sensitive and are unwilling to divulge their experience to third parties.

Recognizing these potential difficulties that might be encountered, early attempts were made to canvass support from the industry. These efforts were primarily focused on briefing operator's safety managers through UK Flight Safety Committee's Maintenance Sub-Committee and CHIRP MEMS group, and concurrent direct approach to selected operators.

UK CAA and CHIRP/MEMS were helpful in providing introductions to potential participants. Initially there was considerable interest from some operators to find out what is involved in this work. Later the interest waned as they begun to realize that the research methodology extended into organizational factors that has a significant impact on the errors at work face, and that causal chain analysis would put managers' roles under scrutiny.

The very nature of CHIRP/MEMS points to the existence of a culture in the industry where occasionally mistakes are covered up by management, employees are not allowed to speak up or formally report mismanagement or error, and employees fear reporting error because of intimidation or threat to their job security. In fairness it should be said that this is NOT the norm for the industry, but the existence of malpractices are known throughout the industry. That is why "safety culture" is an important topic in flight safety or human factors training.

Unfortunately for the research study, other external factors arose that adversely affected data gathering phase. With the onset of economic down turn and "credit-squeeze" started in late 2008, operators considered this type of research for which their support was canvassed were, for them, non revenue generating diversions. Therefore requests for support were not well received. Ironically, it was also a period that investigations on two major accidents put the industry in the defensive and closed their doors to outsiders investigating internal methods.

One was the crash landing of a Boeing 777 at London Heathrow Airport (See Appendix 2) which, mercifully, narrowly missed from becoming a major disaster. The other was the publication of the Haddon-Cave enquiry report[102] that reviewed broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006. These events were not helpful to the study from a data capture viewpoint, but they underscored the importance of research studies of this nature that relate to structured approach to assessment of risk in flight safety.

Although Haddon-Cave report referred to a military aircraft accident under war operational conditions, it focussed on some historical aspects of safety design and safety management of the project at its design, and inception to service, and so casted the limelight over organizational factors that led to the accident. The report was very revealing on the mismanagement and intimidation of staff analysts by managers in authority in order to achieve program timescales and stage payments whilst ignoring detailed design safety issues and requisite investigations[102].

The traditional slow migration of technical staffs and management methods between different employees in aerospace industry, military and civil aviation means such malpractices could well exist in the wider civil aviation industry in UK. They may be the real face of poor safety culture that exists beneath the external veneer that is more attractively presented to the public. It was into such an industrial environment that this research study was introduced, whose prime need was to have free access to safety data and investigations that provides an insight to a company's culture, attitudes and in some cases shortfalls in the processes and regulatory compliance.

While the study made an open invitation to participate to a wide range of commercial operators, nine specific commercial organizations were invited directly to participate in the study, by providing maintenance error data. Six of them were Air Operator Certificate (AOC) Holders. Three were Maintenance, Repair and Overhaul Organizations (MRO). Recognizing the potential availability of good quality data, one defence establishment and a defence industry establishment was also invited.

In the event only 3 organizations responded positively and others were patchy, as summarised in Table 8.1. Some started off well, but withdrew later, offering various reasons for their inability to continue, whereas some others were evasive or if not obstructive. The nature of response or the lack of it may well represent the industry's attitude to this very sensitive subject of human error. Ironically, without their realisation, negative responses were in fact positive data for a study in soft science, as

it is in this case. It enabled the study to assess varying attitudes, culture, sensitivity, secrecy and fears that exist in civil aviation industry.

No doubt all organizations placed safety at highest priority, but when it comes to business the standard statement from senior managers was “Safety? Yes, but not at any cost” implying that there is a financial limit beyond which their safety measures cannot be funded. The impression given was that human error exists and cannot be fully eliminated; operators do whatever is possible to control human error but as a business interest and self protection it is best to keep the lid down and the public to be unaware of the extent of error that prevails in their organizations. Organizations appeared to fear that divulgence of this type of information would make them susceptible to liability claims as well as exposure to poor publicity that might make them less attractive to travelling public.

It was very gratifying that a large operator provided a Director level interview explaining at length their safety policies and attitudes towards regulation, as well as their new directions in oversight. But when it came to sharing data they withdrew access on ground of economy. Another large operator allowed a casual meeting with a Director; but despite their promise, follow up requests were either ignored or blocked. Much later on in the study, when relevant information became available from another source, the researcher realised that he had unwittingly touched on an issue that was sensitive to the airline, of outsourcing C-Checks to a Far East country.

Interestingly, some organizations remained in touch with the progress of the model development and then withdrew support. Some claimed the economic down turn and lack of man power to support our request, but it was also obvious that they, especially the middle managers, were feeling uncomfortable about the concept of investigation along causal chains. Causal chain type analytical investigations would cross normal management boundaries that inhibit progress of in-house safety engineers who are usually subject to local industrial disciplines, despite that they have direct access to AM/CEO.

Transparency of causal chain investigation is generally seen as a threat by middle managers, because where it is correctly due, the model fairly transferred responsibility for errors from the human/ machine interface at the LAE level to organization and management structure. This could be a point of contention and a loss of interest to those managers who usually tend to look for faults with the work force but rarely within themselves.

It was an uphill struggle to get the operators interested into researching into an area which they consider to be very sensitive and guarded. Naturally, the expressed view was that it was commercially sensitive from the viewpoint of competition and that their opponents should not get to know their information. But in reality, from the nature of the discussion and how communications were handled later, it can be inferred that the resistance was mainly for self protection. One very experienced Senior Safety Manager warned that this type of data collection would be detrimental to the business interests of an organization, as underwriters would want to examine the data with respect to declarations and liabilities. In contrast, one airline that supported the study was not only willing to share its data with others, but was also interested in setting up a national data bank and a forum where data could be shared. His main argument was that safety is not a commodity owned by one operator; public would be served better if lessons learnt from incidents are shared with other operators.

Of the 3-organizations that formally agreed to provide data and participate, one regional operator was extremely helpful in the early phases of the study that enabled the design and development of the pilot model. Unfortunately, they did not participate in the full validation trial and failed to respond to requests. One other organization who provided data was an MRO, but it was not possible to obtain a full and consistent set of historic data because they had no access to their clients' aircraft historical data. In the event, the model was validated in only one environment, which provided a comprehensive set of data, without any hold ups or reservations regarding access to data. However, data were released under a confidentiality agreement that data source would be dis-identified and any published report would be desensitized.

Intentionally Blank

Type of Organization	Type of Operation	Initial Approach	Response	Closure Date	Remarks
AOC	Large passenger operator – short, medium and long range - worldwide	Sep 07	Policy level discussion with Eng Director. Withdrew support at GM Engineering Services level, quoting labour shortage.	Jul 09	Economic downturn and inability to provide labour to extract data were quoted reasons
AOC	Large passenger carrier. Long haul - worldwide	Jan 08	Allowed informal meeting with Eng Director, promised to follow up. But repeated reminders were ignored	Dec 08	Eliminated as unwilling to cooperate
AOC- Airline A	Regional passenger operations. Short and medium range	Oct 08	Fully supportive at Director and Safety Manager level. Provided archival data for pilot studies. Complete error history withheld.	Jul 10	Wider data set for validation failed to materialize within timescale
AOC - Operator X	Large air cargo operator world wide	Jun 09	Fully supportive at MD and Safety Manager levels	Jul 10	Provided a full set of data with uninhibited access
AOC	Business jet operator	Mar 09	Initially unresponsive. Eventual meeting with safety manager. Claimed no data in error register.	Apr 09	Self protecting, denying and reluctant data source.
MRO	Maintenance of business jets and large air transport	Mar 09	Expressed a view that MRO not responsible for CAW management. No error records available. Promised to discuss with QM and respond but not returned.	Apr 09	Self protecting and reluctant to provide data
MRO	Maintenance of large air transport	Sep 08	Provided set of data of events within organization. Back up data not available due to aircraft being external customers. Presentation of generic model well received.	Aug 09	Initial set of a data incomplete due to inability to track subject aircraft. Research effort shifted to full set of data from another AOC.
MRO	Maintenance of large air transport	Sep 09	Interviews at Technical Manager and QM level. Could only provide desensitized and abridged results of investigation and no internal reports	Oct 09	Eliminated as an unsuitable data source
CHIRP MEMS Group	Air operators and MROs all types MEMS information sharing committee	Sep 09	Presentation of generic model well received. But non responsive to open request for participation in validation trials.	Jul 10	Unresponsive to open invitation. Variable interest with some members very keen and supportive, and others evasive.
AOC	Large air cargo operator world wide	Sep 09	Correspondence and telephone calls from contact point about difficulties and lack of internal cooperation. Promised interview with Safety Manager; it did not materialize	Apr 10	Eliminated as an unsuitable data source.

Table 8.1 – AOC Holders and MROs invited to participate in validation trials

Intentionally Blank

8.7 Data from Operator X

The Operator X is an Air Operator Certificate Holder, operating large freighter aircraft of modern design, established as one European regional arm of a global network. Its role is to provide serviceable aircraft to meet the transportation requirements of the parent company by pre-positioning aircraft and flight crews at designated locations of the network. The fleet's international routes network covered all of Europe, with some flights going beyond Europe to south and east, and to North America.

At the parent support base, this operator had an integrated maintenance management organization licensed under EASA Part M as well as a Part 145 licensed organization that carried out aircraft maintenance tasks, flight preparations and handling. At outstations, aircraft were maintained by either a third party contractor or another sibling organization of the parent company. In depth Base Maintenance such as "C Check" was undertaken by external service providers, i.e. dedicated MROs.

The services of outstation contractors and MROs were managed through appropriate interface contracts between Operator X and the contractors. Quality of maintenance was subjected to quality audits by Operator X's Quality Audit Department.

UK CAA had a standing responsibility to oversee the Operator X's maintenance organization in order to ensure that they remain compliant with regulation. Furthermore, as an IATA member, Operator X has undergone an IATA Operational Safety Audit (IOSA) that was subject to periodic reviews.

The operator's Safety Department maintained a computer database ("Safety Net") of error incidence and investigation reports for all their aircraft, irrespective of the location where errors were detected, diagnosed or rectified. In addition, it kept records of error incidence on all aircraft handled by the parent base, irrespective of the fact that some of those aircraft belonged to other aircraft operators. Furthermore the Quality Audit Department maintained another database, which stored quality audit findings related to the fleet and to internal and external organizations that maintained these aircraft, as well as UK CAA "Findings "on non-compliance with regulations. Together, these two databases were able to provide a good insight to the way AOC Holder conducted its affairs to ensure that their aircraft were flown safely.

Full uninhibited access to these archives was allowed and it was evident that the organization was methodical, serious and objective, comprehensive and thorough, in setting up these databases. Although Operator X has been in existence for more than 20-years, their Safety Net- based database had been in use for only 26-months at the

time of this investigation. All the available data was released for analysis. Summaries of relevant error occurrences, less audit findings, extracted from the two databases are in Appendix 13, and listings in Table 8.27 and Table 8.28 at the end of this chapter.

From a preliminary analysis of data it was possible to separate relevant information into two groups.

- The first group consisted of those errors encountered on fleet aircraft during their maintenance at any location in the company's route operating network or at the dedicated MROs. With this information for the fleet operation, it was possible to determine the probability of error presence at critical nodes such as Handling & Dispatch, probability of its Consequences and their Cost impact, and finally the Risk. A manager might be able to use this information to gauge how safe the fleet was with respect to the reliability of people who participated in the continuing airworthiness of the fleet.

- The second group are error incidences that either occurred or found by the base station staff on any aircraft that they had handled, i.e. the company's own aircraft and any other visiting aircraft. Therefore this group of error data helps to assess the risk contribution from one specific maintenance organization to any aircraft that it maintained during the relevant period. The probability of a presence of an error on an aircraft at the point of its "release to fly" may be taken as a measure of the reliability of the organization in maintaining continuing airworthiness.

Statistical data derived from the 2-groups are tabulated in Table 8.2 and Table 8.3.

The generic CAW Risk Model, without the air cargo subset, was used for validation because cargo handling error data were not made available. Prior to up taking data, the model was modified as follows:

- Deleted 4 nodes from Operation & Capability. One had no relevance to the operation and the other four were intended to desensitize input data. These were: Aircraft Type& Series RW; Sectors Flown; Operating Role; Destination.

- Added 1 node to Part 21- Part M Interface, namely Pt 21_ Pt M Product Support Contract. Added 2 nodes to QMS exit end, namely: Defence Quality; Consequence Quality. Added 1 node PtM_Pt145 Contract Interface. These were refinements.

The risk model composed of 175 nodes, 204 links and 2,948,941 combinations of parameters, see Figure 8.18, located at the end of this chapter.

Parameter	Jan 08 – Dec 08	Jan 09 – Feb 10	Jan 08 – Feb 10
Sectors flown	16032	18240	34272
Detected errors	3	54	57
Dormant errors	7	63	70
Incidental error lines	10	117	127
CAA Findings L2	6	3	9
QA Findings L2	34	23	57
Total audit findings	40	26	66
Total number of errors	50	143	193
Total lines	16072	18266	34338
Simple error probability x 10E-03	3.111	7.829	5.621

Table 8.2 - Fleet maintenance operations

Taking the 4th column in Table 8.2 that represents the entire period, it can be seen that the fleet has flown 34,272 sectors. During this period 127 errors had been observed of which 57 were recorded as detected. The remaining 70 were dormant errors. A "Detected" error is defined as one that either occurred or observed and reported by personnel. It could be a new occurrence or, if not, a recurring-fault that has been previously misdiagnosed. A "Dormant" error is one that had occurred sometime in the past but remained obscured or undetected, carried into the flight phase unknowingly and later resurfaced and discovered. Some of the errors categorized as dormant errors in this study had been detected by the engineers, whereas other dormant errors have been recognized as a result of the research study. Of the 127 errors, 99 had gone past handling and despatch, takeoff and into the flight; some of these were replication of the same error that either remained undetected or had its root cause unknown and unresolved.

In addition, 64 audit "Findings" had been reported as part of the Quality Audit process as well as 2 "Findings" as part of regulatory oversights. If they were not audit/ oversight inspection "Findings", most likely they would have been transmitted to the flight phase as undetected errors. However in this instance, they were detected and defended, and for the purpose of the research study considered as pro-active error occurrences that were defended.

Statistics for the period 26-months, when categorized into 2 separate periods show that the error records were fewer during Jan – Dec 08. This might have been partly due to genuine reasons of fewer error occurrences, but also it could be due to the reporting system not being properly utilized, perhaps due to unfamiliarity. The MEMS reporting system had been in operation since Yr 2000. But the IT database (Safety Net) had been in use only since 2008. Certainly by 2009, IT base (Safety Net) was

being fully utilized, as evident in the volume of data and distribution. This was the situation for fleet maintenance operations. In the case of base station maintenance operations, error occurrences were fewer and so consistent with the fewer sectors launched from this organization. Therefore the average error probability for base station errors was similar to that for the fleet.

Parameter	Jan 08 – Dec 08	Jan 09 – Feb 10	Jan 08 – Feb 10
Sectors flown	3781	3213	6994
Direct errors	1	6	7
Dormant errors	0	0	0
Incidental error lines	1	6	7
CAA Findings L2	1	1	2
QA Findings L2	14	3	17
Extra error lines	15	4	19
Total number of all error Lines	16	10	26
Total lines	3796	3217	7013
Simple error probability x 10E-03	4.214	3.108	3.707

Table 8.3 – Base station MO operations

8.8 Analysis and uploading

Using data from detailed investigation reports it was possible to determine the primary and secondary causal factors as well as the causal chain, according to the taxonomy established for the model. A few specimen results are at Appendix 13, and the remainder in the spreadsheet.

Results of this analysis were uploaded to separate spreadsheets representing "AOC Holder Maintenance Operations" and "Approved Maintenance Organization Activities". Columns of the spreadsheet represented the nodes of the model. Drop-down menus embedded into the nodes offered parameters against which errors, defences and consequences could be recorded. For the full spreadsheets, see software CD/ DVD, in the Folder titled "Ops X validation", Excel files. See file list in List of Software.

8.9 Input Cost data

Designing a cost model was not within the study's remit, but the study identified elements that might contribute to a cost model. Operators were neither willing to provide cost data nor had any clear idea of how to record cost of error, which usually is considered as part of maintenance cost. Operators did not have explicit human

error cost data. Therefore this study used very rough subjective estimates based on the researcher's experience; without that it would not have been possible to make progress with demonstrating this part of the risk model.

Fortunately, most of the encountered errors and their investigation reports indicated that the investigations themselves were the most frequent outcome from the occurrence. Except for a few cases, corrective actions had been subsumed by routine maintenance; therefore associated cost could not be identified. Similarly, there were no records of consequential costs but rough estimates were made to cost aircraft downtime resulting from the repair or corrective actions.

In order for the study to proceed, estimates were made using a rule of thumb. About one man-week labour was allocated for an investigation, cost £1,000, even though the elapsed time for completion might have taken several months. In most cases, the consequential cost was the loss of use of aircraft for half-a-day, for which £50K was allocated. These values could have been more or less, but as the objective was to prove the concept, the actual values did not matter. If data was made available by the operator, then it would have been possible to allocate them to the right location.

8.10 Results

By compiling the model using uploaded data, probability of error occurrence at each node has been calculated. Separate calculations have been done for data relevant to "AOC Holder Maintenance Operations" for the entire fleet and for one "Approved Maintenance Organization", namely the parent base station. Results of the calculations are stored in each node, and could be read off as required. Refer to software CD for BBN network with compiled input data, Folder "Ops X Validation" BBN files. The calculated probabilities are called "prior probabilities" of error occurrences and they represent the organization's experience over the defined period, i.e. a snapshot of the performance at the end of this timeframe.

8.10.1 Prior probabilities for fleet maintenance

For "AOC Holder Operations" Table 8.4 presents the calculated prior error probabilities for a number of nodes selected from the "Consequences" sub-system as these are the most critical for flight safety. These are in fact critical nodes at the advanced stages of the CAW process before an aircraft is released to service, at the point of its release and the stages before the aircraft takes off. The model has calculated the values No Error Probability and Error Probability, at each node,

according to the data collected during the respective periods. The same information is presented graphically in Figure 8.4 and Figure 8.5, the latter magnifying part of Figure 8.4 representing small probability values. Note that graphs are meant to demonstrate patterns and scales of the range, and not for interpolation.

Status at Key Nodes	Prior Probability Based on Experience %		
	Jan 08 – Dec 08	Jan 09 – Feb 10	Jan 08 – Feb 10
Part M Org			
No Error Probability	99.7	99.7	99.8
Error Probability	0.29	0.26	0.16
Pt 145 Performance			
No Error Probability	99.4	98.7	99.3
Error Probability	0.60	1.32	0.75
CAW Management			
No Error Probability	99.5	98.862	99.3
Error Probability	0.54	1.138	0.66
Release to Fly			
No Error Probability	99.6	98.93	99.4
Error Probability	0.40	1.07	0.61
Handling Dispatch			
No Error Probability	99.3	98.86	99.3
Error Probability	0.66	1.14	0.73
Take Off			
No Error Probability	99.6	99.6	99.8
Error Probability	0.37	0.40	0.24

Table 8.4 – Prior probabilities at key nodes - Fleet maintenance operations

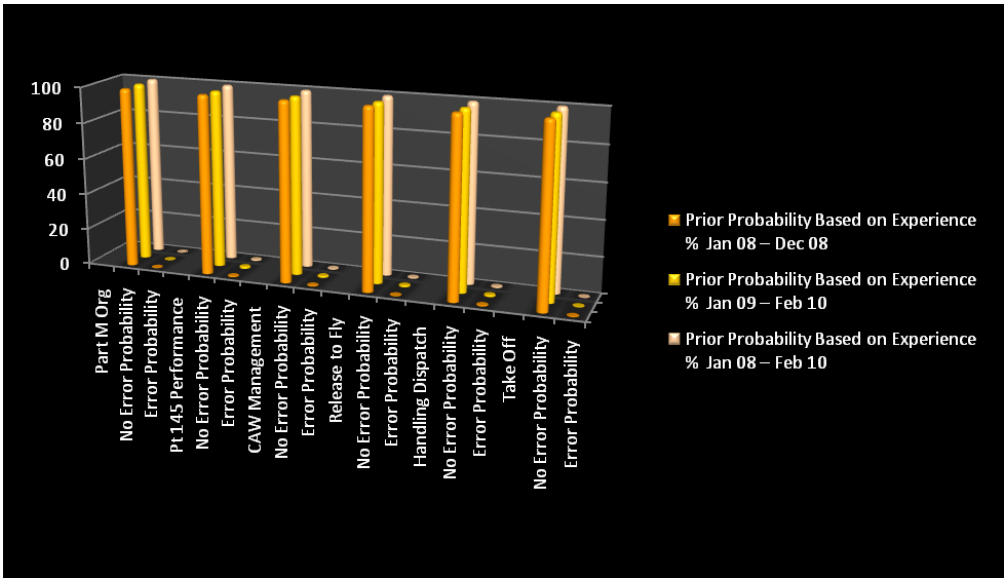


Figure 8.4 – Prior probabilities at key nodes - Fleet operations

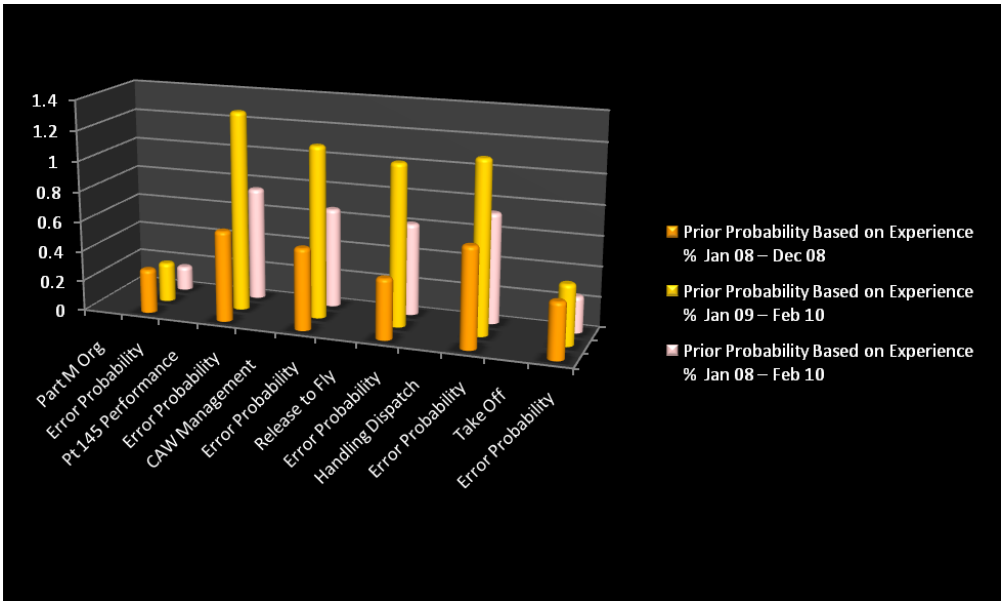


Figure 8.5 – Prior error probabilities at key nodes - Fleet operations

Prior probabilities of incidents occurring during the flight phase based on past experience are shown in the upper half of Table 8.5; the lower half presents probabilities of the monetary consequences of error, i.e. the Cost.

Status at Key Nodes	**Jan 08 – Dec 08**		**Jan 09 – Feb 10**		**Jan 08 – Feb 10**	
	Probability	Risk	Probability	Risk	Probability	Risk
Flight and Consequences	%	£	%	£	%	£
No Error	99.6		99.6		99.7	
Flt Completed Error CF No Cost	0.25		0.38		0.23	
In Flt Shutdown Flt Completed	0.028		0.01		0.005	
Incidence RTB	0.028		0.014		0.008	
Incidence Flt Diverted	0.028		0.01		0.005	
Non Fatal Accident	0.028		0.01		0.005	
Fatal Accident	0.028		0..01		0.005	
Combined Cost (Including cost of disposing detected errors)						
No Cost	98.9	0	97.8	0	98.6	0
Cost group 1 < £10	0.090	0.009	0.20	0.02	0.12	0.012
Cost group 2 < £100	0.094	0.094	0.21	0.21	0.12	0.12
Cost group 3 < £1,000	0.21	2.1	0.33	3.3	0.27	2.7
Cost group 4 < £10K	0.17	17	0.27	27	0.20	20
Cost group 5 < £100K	0.090	90	0.22	220	0.13	130
Cost group 6 < £1M	0.090	900	0.20	2K	0.12	1.2K
Cost group 7 < £10M	0.090	9K	0.20	20K	0.12	12K
Cost group 8 < £100M	0.090	90K	0.20	200K	0.12	120K
Cost group 9 < £1B	0.090	900K	0.20	2M	0.12	1.2M
Cost group 10 < £10B	0.090	9M	0.20	20M	0.12	12M

Table 8.5 – Prior probabilities at key nodes - Consequences and Risk – Fleet maintenance

The rationale for presenting cost of the consequences of error in "Combined Cost" node was given in Chapter Six, Section 6.31. The output from the Combined Cost is the probability of the cost occurring in each respective Cost Group, based on the operator's performance up to that point in time when the relevant data was collected. The results could be used to calculate the risk.

Graphical presentation of data, prior probability of various Flight Consequences, is at Figure 8.6; to improve clarity the indiscernible portion of the graph (i.e. low probabilities) are magnified in Figure 8.7.

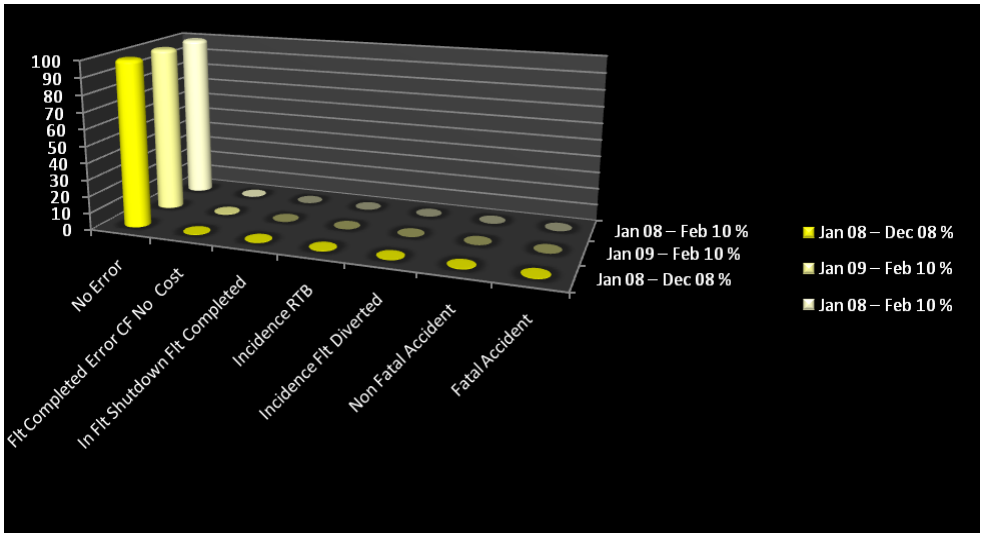


Figure 8.6 – Prior probabilities in Flight & Consequences node - Fleet maintenance

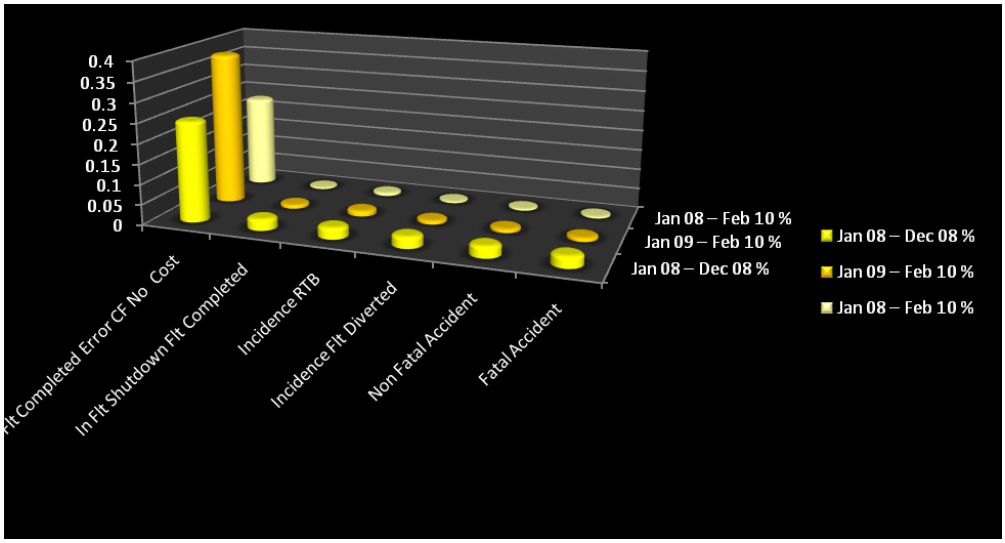


Figure 8.7 – Prior probabilities at Flight & Consequences node - Fleet maintenance

Data for the Combined Cost node are represented graphically in Figure 8.8 and Figure 8.9.

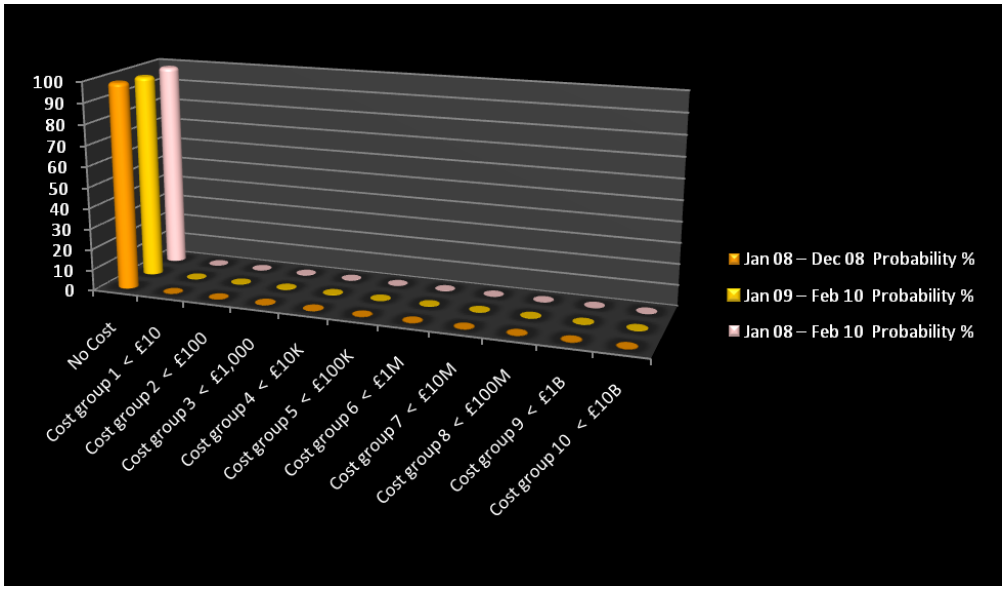


Figure 8.8 – Prior probability of Cost Group Combined Cost - Fleet maintenance

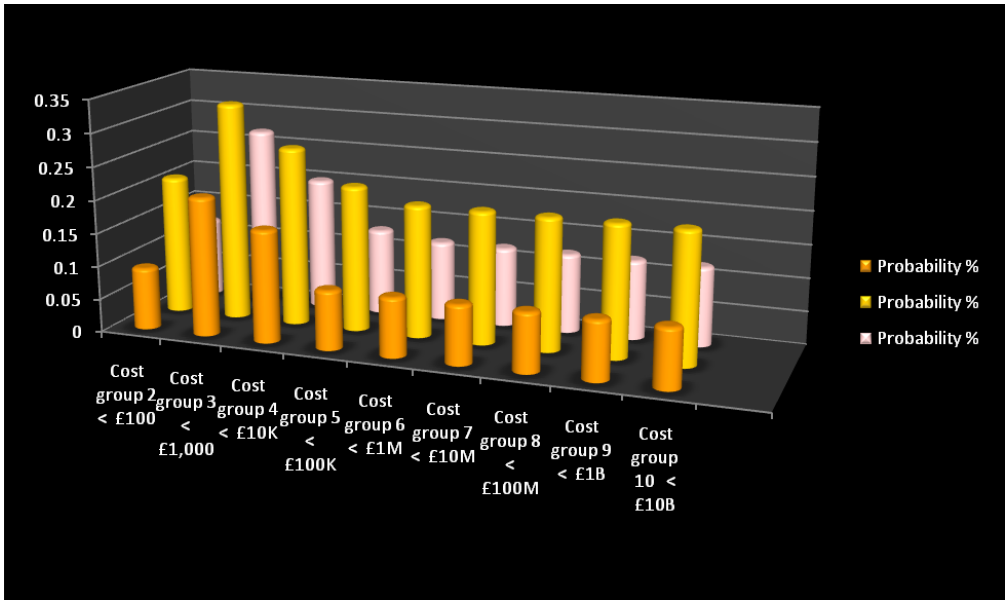


Figure 8.9 – Prior probability of Cost Group Combined Cost – Fleet maintenance

8.10.2 Risk information for fleet maintenance operations

Risk data are presented in Figure 8.10 and Figure 8.11. For clarity, part of the graph Figure 8.10 has been magnified and presented in Figure 8.11.

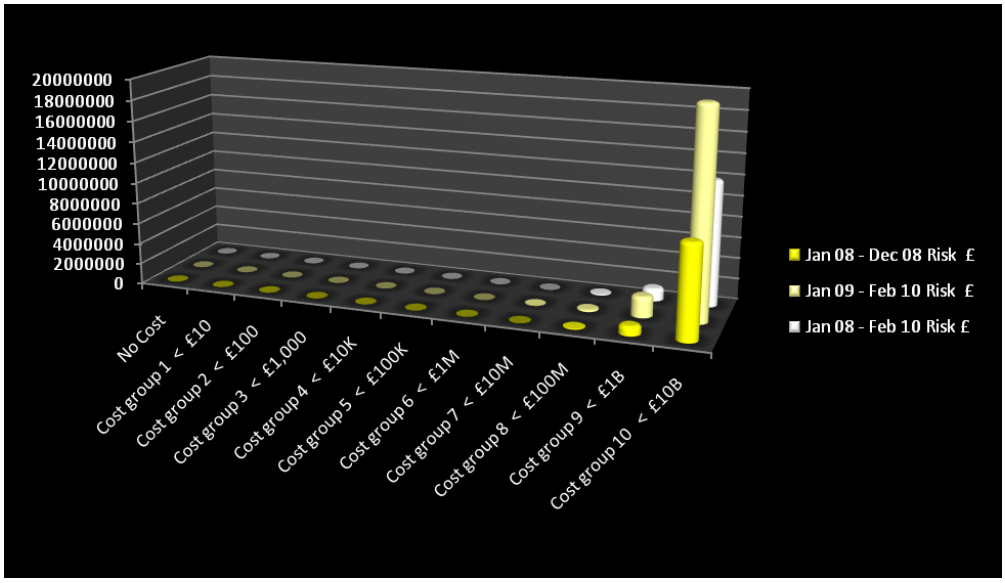


Figure 8.10 – Risk values for each Cost Group - Fleet maintenance

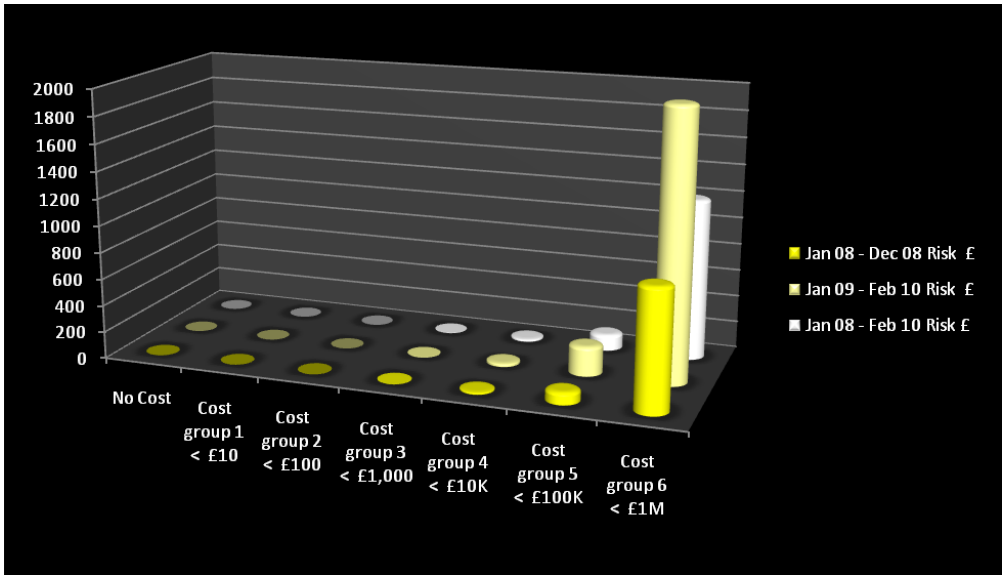


Figure 8.11 – Risk values for each Cost Group - Fleet maintenance

How does one interpret risk data? It is demonstrated below with examples.

For example, if Cost Group 6 is taken, whose upper limit is £1M, the probability of that level of cost occurring as a result of CAW error is 0.12% at the next flight, based on the experience to this point in time when the last set of data was input. This in itself is a risk value. If 1,000 flights were launched at that point, there is bound to be a consequence whose costs would add up to £1.2M. That is one way of interpreting the cost.

The traditional way for calculating risk is, Risk = probability of occurrence x severity of consequences. If this formula is used, the risk value is 0.0012 x £1M = £1200. That means, based on the experience, the next single flight could incur a risk of £1200. How could there be such a cost? There could be different ways. For example, according to the way the costs were built up, there could be an error in the next flight, which if it was detected or, if not, led to a superficial flight incident, could cost the organization about £1200 to investigate and deal with it.

If nothing happened and if it flew next 1,000 flights, one of them might incur a cost of £1.2M for whatever CAW error associated incident, or if not several flights could have errors and incidents whose combined costs would add up to £1.2M. Obviously, if AM/CEO wishes to cover his risk with insurance, then that is the minimum insurance cover that he should obtain. If he is not going to make any changes to his organization, nor update his error experience, and accept this last calculated risk level for the next 1-year and fly 10, 000 flights in one year, then he should anticipate to cover himself for a possible error related cost of £1.2M x 10, i.e. £12M. It seems to be reasonable for typical situations where the costs are imaginable and feasible.

Meanwhile, the lower value Cost Groups too could have probability of occurring, and costs arising as a result. But if those risk values are of a lower magnitude, then AM/CEO need not worry about them, because he has already prepared himself to handle the larger risk at £1M Cost Group 6. In fact for all practical purposes the 3- Cost Groups at the lowest end of the scale can be neglected. They are retained here for reference purposes in order to provide full transparency of the concept development.

However, if one is to cover for the risk of an entire business going into liquidation as a result of a CAW error, and if the business is worth £1B, then the AM/CEO should look at the Cost Group 9. If they wish to cover for that possibility then the potential risk is much higher, because the calculation has put an equal probability of it occurring and increasing liability. Equal probability, because there were not enough data to force the probability down by way of evidence of experience; in its absence, the statistics of the state of nature, in the form of the computer program, has allocated the values of equal probability depending on the known limited evidence and patterns of behaviour. If probability is to be forced down, then more evidence should be collected, or input one's belief that is acceptable to the insurer.

In this model, the provision has been made to deal with Cost Groups going up to £10B, but it does not mean AM/CEO would have to consider taking on those risks, unless he wants to. Therefore the sensible thing to do is to truncate down Cost Groups to what is practical and reasonable, and trust one's luck that the decision was right. If no

cover is provided, then of course, the business would have to be liquidated if something disastrous happens.

Similar situations could arise if a CAW error leads to a major disaster like an aircraft crashing onto population centre. It could happen, but very, very rare because the air space is controlled and thankfully, the CAW system is largely defended.

The model simply demonstrates how and where such costs and probabilities come from. The model gives the rationale. It does not dictate to the AM/CEO what to do. It guides the AM/CEO, and after that, it is up to them to interpret and use the result wisely. More of the equal probability allocation and its magnitude will be discussed later in this chapter.

8.10.3 Prior probabilities for base station

Prior probabilities for the base station are tabulated in Table 8.6, and graphically represented in Figures 8.12 and Figure 8.13.

Status at Key Nodes	Prior Probability Based on Experience %		
	Jan 08 – Dec 08	Jan 09 – Feb 10	Jan 08 – Feb 10
Part M Org			
No Error Probability	98.6	98.3	99.2
Error Probability	1.40	1.68	0.83
Pt 145 Performance			
No Error Probability	98.0	97.4	98.8
Error Probability	1.97	2.60	1.23
CAW Management			
No Error Probability	98.3	97.8	99.0
Error Probability	1.74	2.24	1.03
Release to Fly			
No Error Probability	99.1	98.8	99.4
Error Probability	0.94	1.24	0.58
Handling Dispatch			
No Error Probability	98.2	98.0	98.9
Error Probability	1.79	2.03	1.07
Take Off			
No Error Probability	99.1	99.2	99.6
Error Probability	0.95	0.77	0.40

Table 8.6 – Prior probabilities at key nodes - Base station maintenance

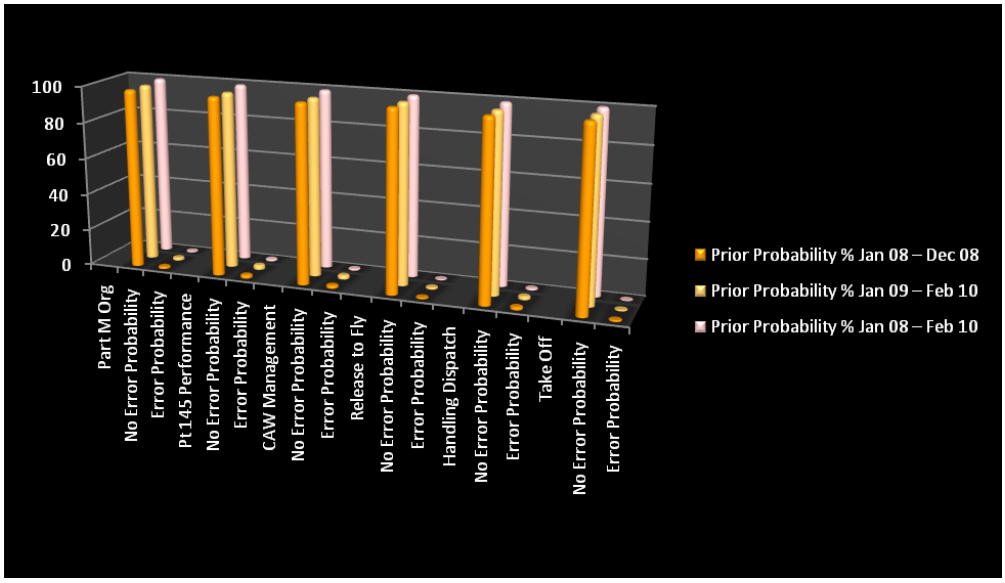


Figure 8.12 – Prior probabilities at key nodes – Base maintenance operations

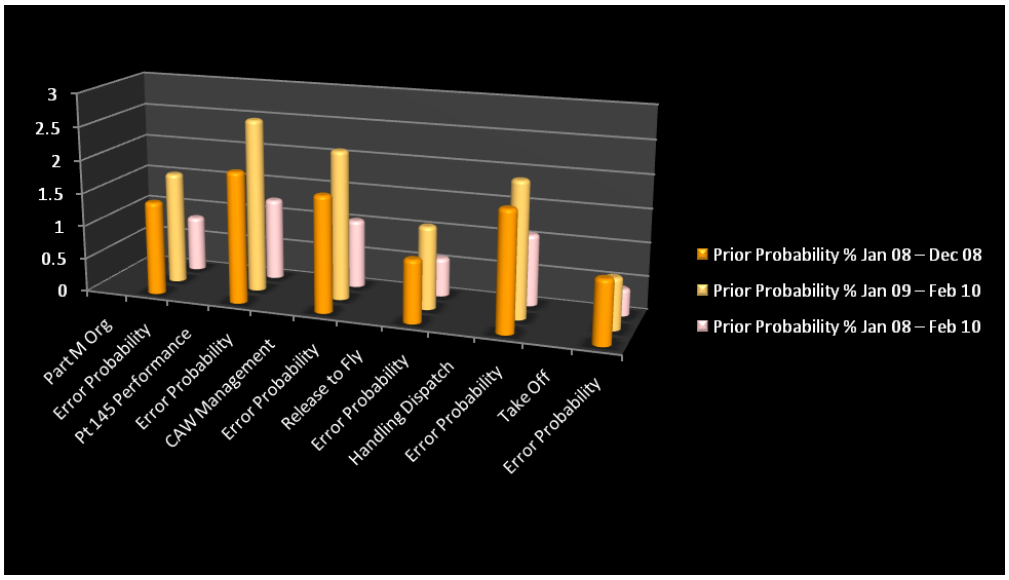


Figure 8.13 – Prior error probabilities at key nodes (magnified) – Base maintenance operations

8.10.4 Flight Consequences and Risk information for base station

For the base station, Table 8.7, upper half presents Flight & Consequences returns; their graphical representation is at Figure 8.14 and Figure 8.15.

The risk values due to error in base station maintenance activities are in Table 8.7 lower half. Interpretation of results is similar to that given in Section 8.10.2.

Status at Key Nodes	Jan 08 – Dec 08		Jan 09 – Feb 10		Jan 08 – Feb 10	
	Probability	Risk	Probability	Risk	Probability	Risk
Flight and Consequences	%	£	%	£	%	£
No Error	99.0		99.1		99.6	
Flt Completed Error CF No Cost	0.16		0.29		0.15	
In Flt Shutdown Flt Completed	0.16		0.12		0.059	
Incidence RTB	0.16		0.12		0.059	
Incidence Flt Diverted	0.16		0.12		0.059	
Non Fatal Accident	0.16		0.12		0.059	
Fatal Accident	0.16		0.12		0.059	
Combined Cost (Including cost of disposing detected errors)						
No Cost	97.2	0	96.9	0	98.3	0
Cost group 1 < £10	0.26	0.026	0.30	0.03	0.15	1.5p
Cost group 2 < £100	0.27	0.27	0.30	0.30	0.16	0.16
Cost group 3 < £1,000	0.39	3.9	0.31	3.1	0.25	2.5
Cost group 4 < £10K	0.32	32	0.42	42	0.24	24
Cost group 5 < £100K	0.26	260	0.30	300	0.15	150
Cost group 6 < £1M	0.26	2.6K	0.30	3K	0.15	1.5K
Cost group 7 < £10M	0.26	26K	0.30	30K	0.15	15K
Cost group 8 < £100M	0.26	260K	0.30	300K	0.15	150K
Cost group 9 < £1B	0.26	2.6M	0.30	3M	0.15	1.5M
Cost group 10 < £10B	0.26	26M	0.30	30M	0.15	15M

Table 8.7 – Prior Probabilities at key nodes - Consequences and Risk - Base station maintenance

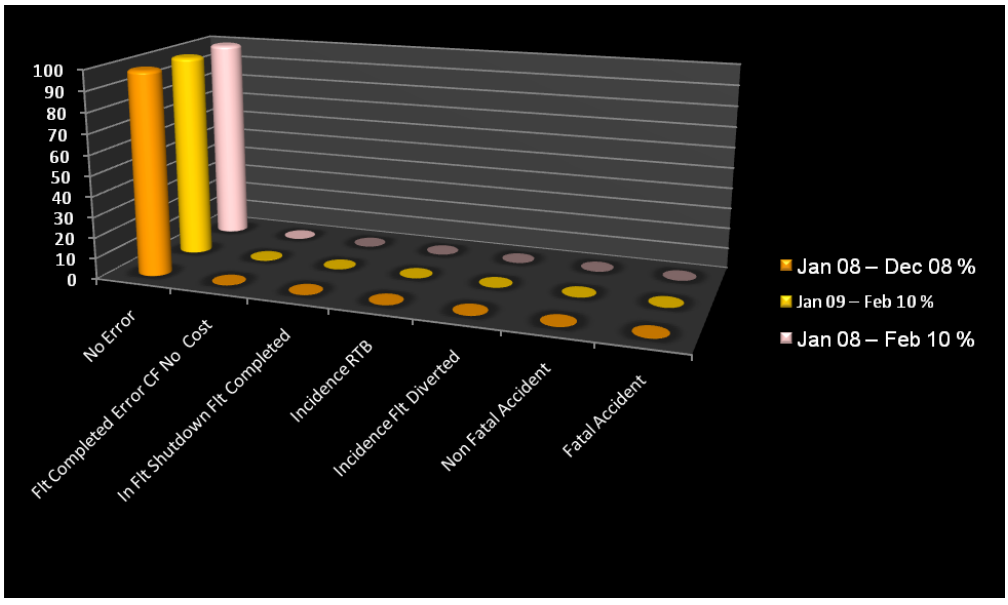


Figure 8.14 – Prior probabilities Flight Consequences – Base station

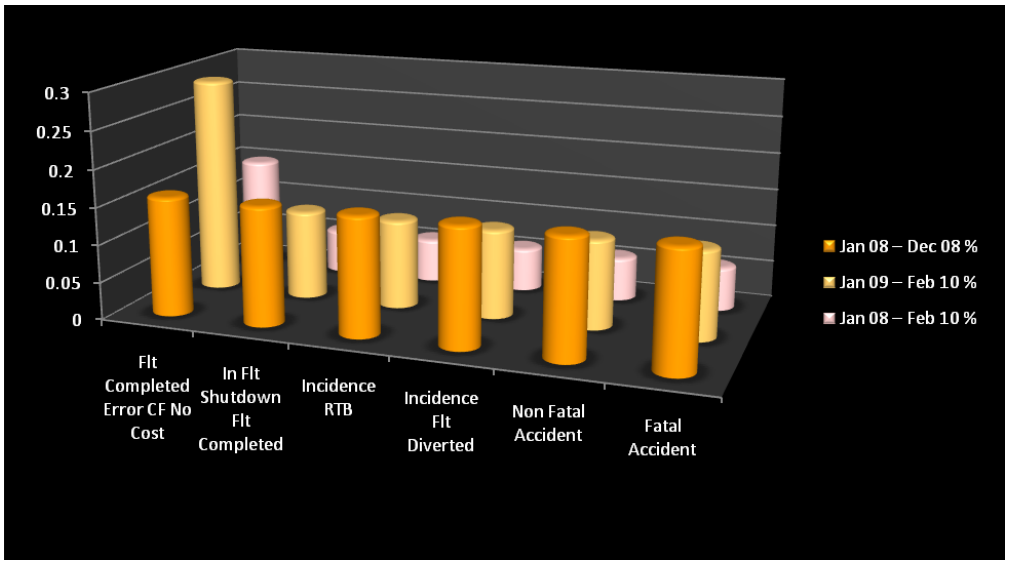


Figure 8.15 – Prior probabilities at Flight Consequences (enlarged) – Base station

8.11 Application

The model could be used to elicit information about the human error issues in the CAW processes of Operator X's fleet operation. For instance given the steady state operations and prior error probabilities, what would be the error probability at Handling and Dispatch if a new error was present at an upstream node, e.g. at Task node, but missed detection. The query could be answered in the inference mode, by setting the Task node, relevant causal factor to 100% and then by reading off the response at Handling and Dispatch, error probability. By setting Task node's causal factor to 100%, the model removes the uncertainty (or confirms 100% probability) of an error present. The model responds by calculating the new probability of error at Handling and Dispatch, i.e. the posterior probability given there was a new error present at another (upstream) node.

Table 8.8 presents a matrix of posterior probabilities at a number of key nodes in response to the presence of errors at upstream nodes. Four examples given:

- Adverse funding decision by CEO which may be construed as an error of judgment.
- Two unconnected errors occurring together Pt 145 AO having problems with personnel and insufficient trade cover under manning.
- Production fault interacting with unsatisfactory AMM, together with failure to update maintenance data.

- Shortfalls in Pt 145 interface contract and shortcomings in Quality Control at work face.

At Handling at Dispatch, error probability has increased from 0.73% at steady state to 17.6%, 24.1%, 22.3% and 11.0% respectively for each of the error incidences listed above.

Status at Key Nodes	Prior Probability %	Posterior Probability %			
		Adverse Funding Decision by CEO	Errors in Pt 145 Personnel + Trade Cover in Manning	Errors in Production + AMM + Data Not updated	Errors in Pt 145 Interface Contract + Quality Control
Part M Org					
No Error Probability	99.8	95.3	91.1	72.5	98.3
Error Probability	0.16	4.67	8.92	2.75	0.16
Pt 145 Performance					
No Error Probability	99.3	74.3	35.3	45.8	47.5
Error Probability	0.75	25.7	64.7	54.2	5.25
CAW Management					
No Error Probability	99.3	86.5	66.9	48.5	73.5
Error Probability	0.66	13.5	33.1	51.5	26.5
Release to Fly					
No Error Probability	99.4	89.0	73.2	58.3	78.5
Error Probability	0.61	11.0	26.8	41.7	21.5
Handling Dispatch					
No Error Probability	99.3	82.4	75.9	77.7	89.0
Error Probability	0.73	17.6	24.1	22.3	11.0
Take Off					
No Error Probability	99.8	96.8	96.8	97.0	98.5
Error Probability	0.24	3.19	3.19	2.96	1.54

Table 8.8 – Effect of Findings 1 – Posterior probabilities at key nodes. Fleet maintenance operations Jan 08 – Feb 10

Through a similar process, posterior probabilities of Flight Consequences have been calculated for the impact of an inappropriate funding decision or a system error triggered by reduced funding level leading to under-manning and shortfall of trade cover. Details are in Table 8.9.

The lower half of Table 8.9 demonstrates the way the risk level changes with new error incidents or, in this particular example, the potential for errors due to reduced funding levels and their impact on risk. In order to quantify the severity of consequences, monetary value of the consequence at Combined Cost has been used. Thus the Table indicates how the probability of certain levels of cost arising as a

consequence of reduced funding levels, given that there has been a past pattern of relationships between finding levels, error and consequences.

The absolute value of the prior probability of risk has been challenged by Operator X, and it has been addressed. The "change of risk" due to change of conditions is in fact more important than the absolute value, because in strategic planning and change management, it is the change of status due to new conditions that needs to be monitored and corrected before the situation gets out of control.

Status at Key Nodes	Prior Probability % (Steady State)	Risk = Probability x Consequence	Posterior Probability % & Risk			
			Wrong Funding Decision by CEO	Delta Risk £	Reduced funds + Personnel in Pt 145 Performance & Trade Cover in Manning	Delta Risk £
Flight and Consequences						
No Error	99.7		97.7		96.8	
Flt Completed Error CF No Cost	0.23		2.21		2.98	
In Flt Shutdown Flt Completed	0.005		0.025		0.33	
Incidence RTB	0.008		0.47		0.63	
Incidence Flt Diverted	0.005		0.025		0.33	
Non Fatal Accident	0.005		0.025		0.33	
Fatal Accident	0.005		0.025		0.33	
Combined Cost (Including cost of detected errors)						
No Cost	98.6	0	94.3		91.1	
Cost group 1 < £10	0.12	0.012	0.43		0.63	
Cost group 2 < £100	0.12	0.12	0.44		0.64	
Cost group 3 < £1,000	0.27	2.7	0.58		0.77	
Cost group 4 < £10K	0.20	20	1.65		2.99	
Cost group 5 < £100K	0.13	120	0.44		0.64	
Cost group 6 < £1M	0.12	1.2K	0.43		0.63	
Cost group 7 < £10M	0.12	12K	0.43		0.63	
Cost group 8 < £100M	0.12	120K	0.43		0.63	
Cost group 9 < £1B	0.12	1.2M	0.43	3.1M	0.63	5.1M
Cost group 10 < £10B	0.12	12M	0.43	31M	0.63	51M

Table 8.9 - Effect of Findings 2 – Posterior probabilities at Consequences and Risk given priors. Fleet maintenance operations Jan 08 – Feb 10

This type of inference resulting from either specific error situations or general trend monitoring could be accomplished through regular updating of the database and recalculating new posterior probabilities. Thus through continual updating, the AM/CEO or their departmental managers and safety managers would have a dynamic risk assessment tool at their finger tip by which they could manage the safety level within their organizations.

Table 8.10 and Table 8.11 respectively provide new posterior probabilities and risk for Parent-Base organization, as a consequence of potential errors occurring at upstream points.

Status at Key Nodes	Prior Probability %	Posterior Probability %			
		Adverse Funding Decision by CEO	Pt 145 Personnel + Performance + Trade Cover in Manning	Production fault + unsatisfactory AMM updating + Maintenance data not update	Pt 145 Interface Contract + Quality Control
Part M Org					
No Error Probability	99.2	74.7	77.3	34.8	99.2
Error Probability	0.83	25.3	22.7	65.2	0.83
Pt 145 Performance					
No Error Probability	98.8	78.4	50.4	53.0	49.2
Error Probability	1.23	21.6	49.6	47.0	50.8
CAW Management					
No Error Probability	99.0	87.1	73.5	50.0	74.4
Error Probability	1.03	12.9	26.5	50.0	25.6
Release to Fly					
No Error Probability	99.4	93.5	86.7	75.0	87.1
Error Probability	0.58	6.50	13.3	25.0	12.9
Handling Dispatch					
No Error Probability	98.9	82.5	88.4	84.7	92.9
Error Probability	1.07	17.5	11.6	15.3	7.12
Take Off					
No Error Probability	99.6	94.1	96.1	94.8	97.6
Error Probability	0.40	5.88	3.91	5.16	2.41

Table 8.10 - Effect of Findings 1 – Posterior probabilities at key nodes given priors. Base station maintenance operations Jan 08 – Feb 10

Once managers learn the way error probabilities at critical nodes, and risk levels behave in response to human error in CAW process, they would want to make course corrections and other improvements to the system. What is the most effective way to do this correction when the system is so complex? The answer lies in sensitivity analysis. Once the objective was identified, e.g. to reduce error probability at Handling and Dispatch, sensitivity analysis would identify those nodes that have the most impact on the Handling and Dispatch node, in order of priority. Corrective actions could be focussed on the higher priority nodes in the ranking. Table 8.12 presents an example of three critical nodes: Combined Cost, Flight Consequences and Handling Dispatch, and the top 10 parameters to which these nodes are most

sensitive. Table 8.13 presents those parameters that have most impact on the Task node for fleet operation and parent base-station respectively.

Following the identification of sensitive parameters, it will be necessary to know which causal factors are most active and therefore should be brought under control. This knowledge could be gained by examining the probability distribution of causal factors within a node. Table 8.14 provides the probability distribution of causal factors in the Maintenance Data node, and Table 8.15 in the Task node. Figure 8.16 is the graphical representation of Table 8.14.

Status at Key Nodes	Prior Probability %	Risk = Probability x Consequence £	Posterior Probability % & Risk			
			Adverse Funding Decision by CEO	Delta Risk £	Reduced funds + Personnel in Pt 145 Performanc e & Trade Cover in Manning	Delta Risk £
Flight and Consequences						
No Error	99.6		89.9		93.2	
Flt Completed Error CF No Cost	0.15		1.0		2.53	
In Flt Shutdown Flt Completed	0.059		1.82		0.85	
Incidence RTB	0.059		1.82		0.85	
Incidence Flt Diverted	0.059		1.82		0.85	
Non Fatal Accident	0.059		2.63		0.85	
Fatal Accident	0.059		1.0		0.85	
Combined Cost (Including cost of detected errors)						
No Cost	98.3	0	88.5		81.8	
Cost group 1 < £10	0.15	1.5p	1.04		1.62	
Cost group 2 < £100	0.16	0.16	1.05		1.63	
Cost group 3 < £1,000	0.25	2.5	1.13		1.70	
Cost group 4 < £10K	0.24	24	1.05		3.50	
Cost group 5 < £100K	0.15	150	1.04		1.62	
Cost group 6 < £1M	0.15	1.5K	1.04		1.62	
Cost group 7 < £10M	0.15	15K	1.04		1.62	
Cost group 8 < £100M	0.15	150K	1.04	890K	1.62	1.47M
Cost group 9 < £1B	0.15	1.5M	1.04	8.9M	1.62	14.7M
Cost group 10 < £10B	0.15	15M	1.04	89 M	1.62	147M

Table 8.11 - Effect of Findings 2 – Posterior probabilities at Consequences and Risk given priors Base station maintenance operations Jan 08 – Feb 10

Rank	Combined Cost		Flight Consequences		Handling and Dispatch	
	Sensitive to error at	Sensitivity Index	Sensitive to error at	Sensitivity Index	Sensitive to error at	Sensitivity Index
1	Consequences Pt 145	0.02039	Take Off	0.02373	CAW Management	0.01340
2	Defence Pt 145	0.01951	Defence Pre Take Off	0.01062	QMS	0.00964
3	Consequences Handling & Dispatch	0.01699	Consequences Pre Take Off	0.01034	Defence Handling & Dispatch	0.00830
4	Handling & Dispatch	0.01686	Handling & Dispatch	0.00424	Consequences Handling & Dispatch	0.00809
5	Consequences Pre Take Off	0.01655	Release to Fly	0.00134	Pt 145 Performance	0.00598
6	Flight and Consequences	0.01370	CAW Management	0.00108	QA Performance	0.00452
7	Take Off	0.01283	Quality Management System	0.00079	Task	0.00384
8	Consequences Quality	0.01216	Defence Handling & Dispatch	0.00068	Pt 145 and Pt M Compliance	0.00376
9	Defence Quality	0.01114	Consequences Handling & Dispatch	0.00066	Defence Pt145	0.00284
10	Pt145 Pt M Compliance	0.00907	Pt 145 Performance	0.00047	Consequences Pt 145	0.00274

Table 8.12 – Sensitivity of 3-key nodes to other parametric changes - Fleet maintenance

Sensitivity of Task to Errors at Other Nodes				
Ranking	**Sensitivity**	**Base station**	Fleet	**Sensitivity**
1	0.07075	Attitude to Task	Attitude to Task	0.0229
2	0.05414	Task Management Docs	Pt145 Org Performance	0.02063
3	0.05258	Pt145 Org Performance	Task Management Docs	0.01858
4	0.05247	Workface Stress	Workface Stress	0.01687
5	0.04801	Facility Environment	Logistic Support	0.01531
6	0.04703	Maintenance Data	Facility Environment	0.01474
7	0.04666	Tools And Test Eqpt	Maintenance Data	0.01442
8	0.0464	GSE	Tools And Test Eqpt	0.01405
9	0.04407	LRU Spares	GSE	0.01362
10	0.04202	Logistic Support	Manning	0.01287
11	0.04064	Manning	LRU Spares	0.01268
12	0.02517	CAW Management	Corporate and Policy	0.00749
13	0.02431	Corporate and Policy	Individual Traits	0.00587
14	0.0127	Individual Traits	Logistic Support Policy	0.00279
15	0.00967	Part M Org	Eng Ops Policies	0.00246
16	0.00935	Logistic Support Policy	Commercial Policies	0.00231
17	0.00847	Eng Ops Policies	Certification Recertification	0.0022
18	0.00834	HR Policies	HR Policies	0.00216
19	0.00773	CEO AM Decisions	CEO AM Decisions	0.00207
20	0.00754	Commercial Policies	Pt M Pt145 Interface	0.00172
21	0.00705	Pt M Pt 145 Interface	Change Management	0.00136
22	0.00614	Certification Recertification	Tech Knowledge Skills	0.00116
23	0.00458	Change Management	Flt Ops Policies	0.00105
24	0.00397	Flt Ops Policies	Pt M Pt145 Contract	0.00096
25	0.00352	Tech Knowledge Skills	Global Factors	0.00046

Table 8.13 – Sensitivity of Task node error to causal factors

Maintenance Data Node	Probability - %
No Error	99.7
Inadequate or unavailable	0.049
Not updated	0.037
Poor access to data	0.032
Unavailable at workface	0.031
Conflicting data	0.031
Information not used	0.029
Incomprehensible	0.026
Incorrect data	0.026
Incorrect amendment	0.026
Ambiguous	0.026
Confusing graphics	0.026

Table 8.14 - Example of probability distribution of causal factors at one node - Fleet Operation

Task Node – Types of Error	Probability of Error
No Error	0.99314000
Installation error	0.00072866
Poor maintenance practice	0.00072262
Poor or incomplete diagnosis	0.00066641
Inattention damage	0.00064765
Poor inspection or test standard	0.00059209
Misinterpretation of data	0.00055062
Approved data not followed	0.00052496
Unrecorded work	0.00052168
Servicing error	0.00050657
Work uncertified	0.00047141
Missed independent checks	0.00046378
Certified without verification	0.00046378

Table 8.15 – Probability distribution of error at Task node (high resolution)

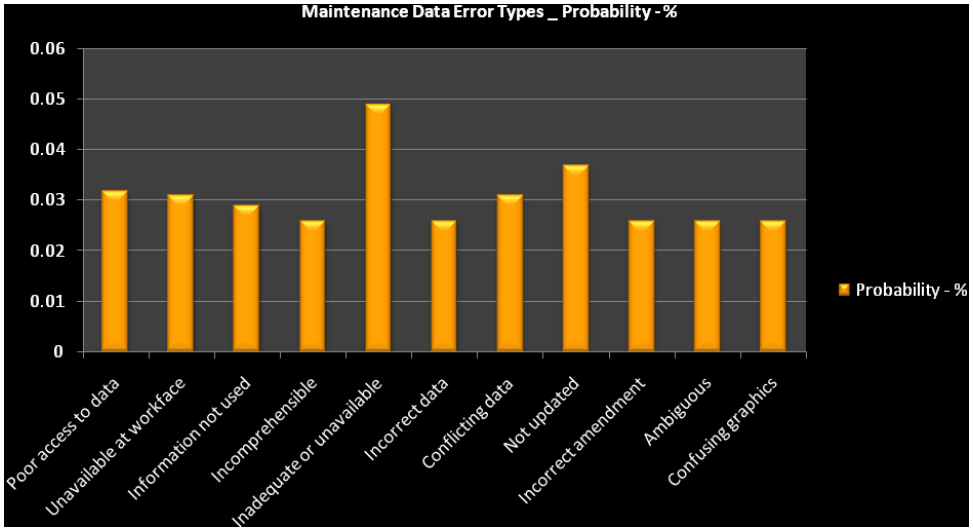


Figure 8.16 – Probability distribution of causal factors in Maintenance Data node

8.12 Operator's belief

Referring to "Combined Cost" Operator X made an observation that they would be more interested on the error probability at the end of the CAW process, and what the potential flight consequence was, rather than risk level as calculated at Combined Cost. The idea of putting a cost to fatal accidents was not well received.

During the follow up discussion it emerged that part of the objection was rooted in the idea that "human lives" would have to be costed as if they were a commodity for the purpose of measuring severity of consequences. Obviously, it is unacceptable to public sensitivity and an organization or concept that tries to pre-empt their potential

liabilities would be seen as uncaring in the public eye. Harmonizing with the Operator X's sentiment on this point, the study too has been hitherto advocating the use of probability at Flight Consequences as a suitable measure, keeping Combined Cost data as back up information.

However, in trying to take out the emotion from a problem- solving type research assignment, it was necessary to adhere as closely as possible to already established conventions. For that reason, the entity risk was presented in the traditional way. This calls for a cost to be assigned to the loss of human life, or alternatively the value of saving a human life, and the study has taken the practice set by insurance underwriters. It is recognized that actuaries place a cost to "loss of life" for insurance and legal purposes. This study did not attempt to value human life, but simply place a cost band that might be adequate to cover loss of human life as well as other material assets.

Operator X further challenged the results for "Flight Consequences" results stating that the prior probabilities of major and fatal accidents as derived by the model were unacceptable to them. This figure was 0.005 per cent for fatal accident, i.e. 5×10^{-5} which the operator claimed was unacceptably pessimistic and that at that rate the operator would have no option but to close down their operations.

The operator also queried the rationale for equal probabilities between fatal accidents and non-fatal accidents, stating that these values would not be so in real life. Referring to global figures, they claimed that there would be a more skewed profile, which the study interpreted as one resembling the trailing end of a log-normal distribution curve. The operator claimed that they maintained global safety standards and therefore, it would be reasonable to apply global accident rates to their organization, whereas the figures computed by the model were widely out from the global standards. They wanted to know if the model could be modified to match global experience that they consider as their prior error probability.

This challenge was not surprising as it followed a natural phenomenon called, "Representativeness", which is a collective term used to describe a range of fallacies that people make when making subjective assessment of probabilities[103] In this particular situation two of the fallacies that came into play were insensitivity to prior probabilities and insensitivity to sample size.

In insensitivity to prior probabilities the subject gets misled by past patterns to form a stereotype image of the performance. It ignores the fact that the next event could fall

outside the pattern and at that point all other possibilities as well as that of the previous pattern are possible. The other fallacy, insensitivity to sample size, ignores the principle that a large sample is more likely to converge to the universal mean and that a small sample size could produce a wider scatter from the mean.

Nevertheless, in order to address Operator X's concerns, the model was rerun using an alternative, simulated data file representing Operator X's belief. The following sections outline the approach taken, data used and the results.

8.13 Global experience

Global experience in the safe operation of commercial air transport is published in IATA Annual Safety Report in the form of statistical data on fatal and major accidents world-wide. The actual values vary from year to year, but in general there is evidence that the overall fatal accident flat-rate has levelled off around 0.7 per million sectors; the lowest level published was 0.65 fatal accidents per million flights for western built passenger jets according to IATA[20.]. In contrast world-wide cargo aircraft experience 4 times as many fatal accidents as of passenger aircraft.

The overall global rates are composed of a mixture of regional variations operating to different regulations, and relating to jet and turbo prop aircraft of different makes, age, technology and weight categories, as well as of manufacturing base. IATA data was limiting however, because they do not contain information on less severe consequences.

Data for UK civil aviation accidents had a slightly better resolution, and therefore it was decided to use UK experience in this analysis instead of global experience. On reflection, UK national experience was more appropriate for this operator, as they were regulated by UK Civil Aviation Authority. The UK rates for achieved safety level were numerically better (i.e. lower accident rate) than the global rates.

Moreover, this AOC Holder operated a fleet of aircraft (Type 1) and (Type 2), which had proven high safety performance standards applicable to western-built passenger jets, even though they were used as cargo aircraft. Evidence from US supports the view that large cargo carriers operate to similar safety standards as that of passenger carriers[104]. In the UK, there was no evidence to suggest that cargo aircraft were less airworthy than passenger aircraft nor operating in environments as in North America or in Africa. It was known that the most aircraft from AOC Holder's fleet were aged 23-26 years, but they have not had any accidents. Except for the fact that they were in cargo role, they were regulated to the same EASA standards as applicable to

passenger jets. All this evidence justified the application of the achieved UK national safety standard to this operator, according to their belief, irrespective of the error performance observed for the period taken for the validation trials.

8.14 Data for UK achieved safety level

Raw data on UK experience, as used in this study, came from UK CAA Published report CAP 780[6]. Some gaps in CAP 780 data, especially those relating to low severity consequences that were not usually covered by MOR, have been filled with data from UK CAA Paper 2009/05[105.] The latter is an updated revision to CAA Paper 2007/04[53]. Relevant data are tabulated in Table 8.16.

Period of flying	1998-2007 CAP 780 Data	
Sectors flown	10.899M	Rate per M sectors
Reported accidents	132	12.1112
Fatal accidents	5	0.458758
Non fatal accidents	127	11.652445
Serious incidents	155	14.22
MOR Occurrences	42,000	3853

Table 8.16 - Raw data- UK experience for 10-yr period 1998-2007

CAP 780 data represented all incidents attributed to a full range of causal factors, mostly falling outside the domain of maintenance and CAW processes, e.g. flight operations. In estimating the proportion attributed to maintenance related human error, 15% of the full values were taken, given that historic evidence indicate that that 6-15% of all flight incidents are attributed to maintenance related errors[6,7,8].

There was no exact match between the categories of consequences as used in CAP 780 and those categories used in the CAW Risk Model. Table 8.17 Columns 2 and 3 summarize the way available evidence from CAP 780 were categorised. These were in turn remapped against the list of consequences used in the model, Table 8.17, Columns 4 and 5. Column 2, lists an ideally desired categorization for a much improved resolution, whereas Column 3 demonstrates the wide-cut method adopted by CAP 780. Column 4 lists the categorization as used in the CAW Risk Model. Column 5 is the way this study spread the known evidence given in block-figures to a distribution using the well known 1 in 600 rule[31] for an error-pyramid. That is the best the study could do with a scanty set of data to create a “Belief-Based” incident distribution

	Desirable distribution of flight consequences	Estimates per M sectors	Categorisation used in the model	Case files used in the model/M
1	Flights believed to be clear of CAW errors. No flight incidents	Remainder of 1M	No Error	Remainder
2	Flights carrying known or detected errors, but authorised to fly	NA	Flight completed. Error carried.	531
3	Flights carrying missed or dormant error, identified after an investigation, but had no flight incidents	NA		
4	Flight incident, but flight completed as planned	578 incidents		
5	Flight incident en route, aircraft diverted		Incidence. Flight diverted	53
6	Error found after take-off, aircraft returned to base		Incidence RTB	10
7	Flight incident, engine shutdown		In flight shutdown. Minor non fatal accident	5
8	Minor accident with or without fatalities	2.133 serious incidents		
9	Major accident with or without fatalities	1.75 non-fatal accidents	Major accident	1
10	Catastrophic invariably with multiple fatalities	0.06881 fatal accidents	Fatal accident	0

Table 8.17 – Mapping Probability distribution - UK experience

The above distribution was simulated in an input case file for the model. Initially, the test file represented one-million sectors, later expanded to three-million sectors, with pro rata increment of the number of consequences, and eventually to 6M. Table 8.18 presents a breakdown of the input files used.

Category of consequence	Validation trial	Simulated data files representing UK rate			Prior data plus real data
No of lines/ sectors	34338	1M	2M	3M	3.034338M
No error	34239	999400	1998800	2998200	3032439
Flight completed- error carried	98	531	1062	1593	1691
Incidence- flight diverted		53	106	159	159
Incidence RTB	1	10	20	30	31
In flight shut down		5	10	15	15
Major accident		1	2	3	3
Fatal accident		0	0	0	0

Table 8.18 – Input simulated case files and real case files from Operator X's validation trial

8.15 Interpretation of the results from simulation

Conditional probabilities calculated at the Flight & Consequences Node are tabulated in Table 8.19, Columns 3, 4 and 5, for case files containing 1M, 2M and 3M sectors respectively; these are the priors based on Operator X's Belief. Then Column 7 would be considered as the posterior when a prior (based on Belief) is updated by superimposing real data. Results in Columns 3, 4, and 5 can be compared with the results of the validation trial (Column 2), as well as with the posterior probabilities when prior probabilities were updated using real life experience (Column 7). They exhibit the phenomenon of the results converging to a universal mean as the population size increases.

Category of consequence	Validation trial	Simulated data files representing UK rate				Prior data plus real data
No of lines/ sectors	34338	1M	2M	3M	6M	3.034338M
No error	0.99742	0.99932	0.99934	0.99935	0.99933	0.99935
Flight completed- error carried	0.002300	0.00059447	0.00057937	0.0005743	0.00057395	0.00057794
Incidence- flight diverted	5.21E-05	6.1239E-05	5.8768E-05	5.7946E-05	5.96E-05	5.495E-05
Incidence RTB	7.50E-05	1.3271E-05	1.1936E-05	1.1496E-05	1.1532E-05	1.1254E-05
In flight shut down	5.21E-05	7.6932E-06	6.4901E-06	6.0946E-06	5.9423E-06	5.7916E-06
Major accident	5.21E-05	3.231E-06	2.1337E-06	1.7736E-06	1.4708E-06	1.6951E-06
Fatal accident	5.21E-05	2.1155E-06	1.0445E-06	6.934E-07	3.5297E-07	6.7093E-07

Table 8.19 - Probability distribution of consequences – Simulated prior and posterior based on updating the belief with real data

That aside, this exercise has principally demonstrated that it is possible to initialize the model by simply uploading it with a prior probability distribution of consequences, in this case a flat rate based on the UK commercial transport achieved safety level. But, the trial confirms that the operator would have to pretend having had at least 3M sectors of experience to verify that the model returns a value resembling the UK flat rate for major accidents, 1.75E-06 (Table 8.17 Column 3); the conditional probability rate returned was 1.7736E-06. Exact match could not be expected, because the input UK rates are flat rates (i.e. arithmetic averages) whereas the output values from the model are conditional probability values. Errors would be due to the way the incident distribution profile was created (Table 8.17, Column 5) but these errors are unquantifiable at this stage of the research study. It is recognized that some errors are there, but the principle of "Representativeness" (See Section 8.12) has been demonstrated, which is the lesson to be learnt here.

When 34,338 sectors of Operator X were superimposed on a UK standard rate profile, the model computed rate for major accidents turned out to be 1.6951E-06, which is in fact better than the UK rate.

At 3M sectors, based on conditionality, the model returns a total of 74 incidents per million sectors, composed of flight diversions (57), return to base (11) and in-flight shutdowns (6), against the UK rate of 68 per million based on flat rate.

Interestingly, the fatal accident conditional rate returned after 3M sectors is 6.934E-07, resembling the global fatal accidents flat rate of 0.7 per million, or the lowest recorded 0.65 per million hull loss rate for western built jets in 2006[20]. When 34,338 sectors were superimposed, Operator X's rate for fatal accidents turned out to be 6.7093E-07 or 0.67 per million.

After 6M of simulated sectors, fatal accident rate dropped to 0.353 per million (=3.5297E-07), which was close to 0.459 per million UK national rate; there were 5 actual UK fatal accidents, in 10.889M sectors (=0.459 per 1M).

These figures are consistent, providing confidence that the mathematical calculations, statistical concepts and technique used by the model are reasonable. By inference, it confirms that the logic and architecture of the model are also correct.

Referring to Table 8.19, last column, it is interesting to note that when 3M simulated sectors were updated with Operator X's 34,338 sectors, the posterior probabilities turned out to be smaller than the operator's belief. If the Regulator were to accept the Operator's claim that they were operating to global (or if not UK) safety levels, then the follow on result confirms that the safety performance of the operator is now better than his belief, despite the significant number of observed errors for the period concerned.

One explanation to this apparent dichotomy lay in the "Defence" activities. As long as any detected errors are successfully defended by CAW staff, or their effects are intercepted by flight crew to prevent them turning out to be incidents, then the Operator and the Regulator could remain content that errors are managed and flight safety is maintained. Design safety features and sheer chance (or luck, as some people call it) also would have helped to maintain the dynamic balance of risk level.

Finally, does this simulation confirm the Operator's belief that they were operating to global (or if not UK) safety levels? No doubt it is operating to global standards, but whether it achieving the global level of safety is debatable and should be left to the Regulator to decide on the basis of evidence and results. The superimposition of actual experience on a prior belief of operating to global (or UK) safety standard returned Operator X's desired result. That is because the 34,338 that the operator has produced as its experience is dwarfed by the 3M sectors used to simulate the claim that they were operating to global safety level. If the 3M simulated sectors represent their (previously unrecorded) experience, say over 40-years, then their claim is justified.

This means, if the operator has already been achieving global safety level, then a 2-yr period of glitch is not significant if it is viewed from a strategic perspective. The trend has already been set and robust, and an excursion from the trend need not create an alarm. However the excursion ought to be reviewed against the contributing data, and then monitored to ensure that it does not set a new diverging trend, in which case there would be a safety risk. That is one side of the argument.

On the other side, there might be a different interpretation as explained below.

8.16 Alternative interpretation of results

From a statistical viewpoint, an operator might not be able to claim the global rate of probabilities on the basis of their following EASA procedures alone, if in reality they have not generated a large enough experience to justify the claim. The only way they could claim the global rate was if they had flown sufficient numbers of sorties over an extended period of time equivalent to global rate, say at a rate of one million sectors in one year, which a very large operator might fly.

It is not surprising that an operator wishes to claim the merits of the global experience because they belong to the same club as all other operators who operate aircraft safely to regulation. But it may unreasonable to claim the data that belong to the group as belonging to each member for their use, unless they have their own individual experience to justify that claim. Statistically the collective group data does not belong to one member. If they try to use it, then they are trying to usurp an achieved level by the group that cannot be individually justified.

Quoting one example, how could an operator justify high standard, if they have flown an aircraft 28-times consecutively with a loose article next to engine and flap controls. If a passenger knew of this situation, would he have considered it safe to travel in this

aircraft? Most likely, the answer is no. In this instant, no flight incident took place, and that was most likely down to luck than to any finesse in the way aircraft was maintained or the way it was designed. Bad weather or another condition requiring an abnormal manoeuvre could have dislodged the loose article leading to a potential incident. The fact that nothing happened should not be construed as credit to the safety standard of the operator. In fairness to the operator, in this particular case the outcome categorized as "No Flight Incident" by this study as it was upholding the principle that only actual experience would be input.

If the study adopted the ICAO definition of risk (Section 3.3), the potential consequence could have been categorized as a potentially major accident, or even worse, the loss of an aircraft in a worst foreseeable scenario. In that situation, under the threat of this possibility, would not an AM/CEO have grounded his fleet until the offending aircraft and loose article was found?

On querying about this incident by the researcher, the operator quoted the maintenance procedure, stating that there was no need to inspect the engine nacelle repeatedly. Moreover they stated that once the original error was admitted as erroneous, then that should be the end of the error incident and that all other subsequent sectors flown were safe, as nothing happened during those sectors, and that there was no regulation to cover unknown conditions. But the fact remains, that those sectors were potentially unsafe from a flight safety point of view. That is, given the nacelle inspection was inadequate in the first place and the control of disposable stores had not been properly done, if the first sector flown after maintenance was unsafe, then all other sectors flown after that were also unsafe. The cover provided by the rules or, more correctly lack of rules, had no meaning and no value, if in the event the presence of the loose article had caused an accident during any subsequent flight.

Whilst the primary cause remained as the inadequate loose article check after the maintenance task, there were other contributory factors. These were the failure to account for the items taken to the aircraft and unsupervised work under time pressure during unsocial hours. Thus on the question of safety, Operator X should respond to it objectively with safety in mind, rather than with rules in mind.

Given this type of situation, where the real safety is missing but apparent safety by manipulation of rules exists, the Regulator can anticipate an operator making this type of claim in order to safeguard their market position, commercial and legal interests. However, analysis based on BBN relevant to the trial period in which data was collected, suggests that claimed safety based on adhering to rules and procedures alone would not suffice.

This example demonstrates and provides the proof for misrepresentation of safety through normal practice as followed by operators and the Regulator under the present rules-based safety assessment, which is process driven even though the rules have been written objectively. The process, and the local disciplines that convert the rule to an action, failed to deliver the objective. They might go parallel most of the way, but whenever specific cases as this example are examined, it can be seen that true safety had diverged from apparent safety.

This analysis leads us to consider using risk level based on the organizations real safety performance rather than on their belief on account of their claim to adhering to EASA or other regulation. The proof of the claim is in the performance, and not in the belief.

Thus, the Regulator might grant a license to a new operator to undertake an operation on account of their meeting EASA Regulation as a minimum requirement, as it does at present. But when it comes to routine monitoring, a new, previously unknown operator might draw more attention, closer supervision and more detailed audits and oversights, to reflect its own history, experience and performance. The Regulator may subjectively judge the situation pessimistically until the reliability and integrity of its operations is proven and remains consistent over a longer period. A large airline that usually flies about 1M sectors or more per year that has consistently shown safe performance would fall into a safer category justifying fewer or less frequent oversights.

8.17 Compromise between the two interpretations

Given the foregoing two interpretations how should the Regulator determine and select a suitable course of action? Should they opt for the risk level calculated on the operator's belief that it was operating to global safety standards, superimposed by actual experience over a short period (Method 1), or the risk level calculated for the actual experience alone (Method 2)?

The recommendation from the study is that the former (Method 1) should be used for determining risk level from a strategic viewpoint, and that the latter (Method 2) should be used from a tactical viewpoint. Since the operator is responsible for the day to day airworthiness and flight safety issues, they should pay attention to the way risk levels change with routine occurrence of errors. If they do not follow this line, but fall back on the strategic and long term risk levels, then they would be undermining their readiness and alertness necessary to maintain high safety standards.

Strategic risk levels based on global levels superimposed with actual experience could be used by the Regulator as a performance indicator to help implement RBO concept.

8.18 Risk based on Combined Cost

There was no Global or UK standard probability distribution of cost due to accidents. IATA usually publishes Air Claims provided cost data annually but even they comprised of block figures for fatal and major accidents; the figures fluctuate wildly from one year to another. However using IATA historical data, it was possible to estimate that the maintenance error contribution to the cost of their consequences was around £6M per 1M sectors, i.e. flat rate at 15% of the total cost. The researcher's intuition based on professional experience is that this estimate is too low. Even if this figure was doubled to account for the cost of unreported incidents, it amounts to £12M per million sectors, attributed to human error in maintenance. The £12M cost was spread out amongst 600 error lines as in Table 8. 20. For the computer run, the UK cost break down per million sectors flown was assumed to be the same as for global cost breakdown.

Cost Group	Value Lower Limit (£)	Sectors	Total Cost (£)
No Cost	0	60	0
1	1	0	0
2	10	0	0
3	100	202	202,000
4	1,000	312	3,120,000
5	10,000	20	2,000,000
6	100,000	6	6,000,000
7	1M	0	0
8	10M	0	0
9	100M	0	0
10	1B	0	0
Total		600	11,322,000

Table 8.20 - Cost distribution profile

Table 8.21 presents the probability values returned by the model for each cost group for Operator X's direct experience (34,338 sectors), for 3M simulated sectors of UK safety level flying, and finally for 3.034338 M sectors, i.e. simulation updated with Operator X's own experience. Risk values have been manually calculated and inserted alongside with the probabilities for each Cost Group's lower limit.

Column 2 of Table 8.21 demonstrates that the high incident rate for the period concerned is associated with a higher risk level than expected from operating to global rate at Column 4, but if viewed from a long established trend, the excursion should not create undue alarm. This is similar to a well proven safe driver placing an insurance claim in one year because he had a minor accident. One or even two claims would not necessarily make him a high risk, provided of course he has already paid to cover his no claims bonus protection. In fact the last two columns of Table 8.21

suggest that, against its strategic position, Operator X was doing quite well in further reducing the overall risk due to CAW human error. Thus the delta risk, i.e. the change of risk and magnitude becomes performance indicators, suggesting that Operator X is doing well in reducing risk. Again the explanation lay in the defences and error management mechanism that has been in force during the period concerned.

Status at Key Nodes	34,338		3,000,000		3,034,338	
	Probability	Risk	Probability	Risk	Probability	Risk
Combined Cost (Including cost of disposing detected errors)						
No Cost	0.98565	0	0.99772	0	0.99766	0
Cost group 1 < £10	11.941E-04	0	2.2819E-04	0	2.2654E-04	0
Cost group 2 < £100	12.43E-04	0.01	2.2819E-04	0	2.271£-04	0
Cost group 3 < £1,000	26.74E-04	0.12	2.2819E-04	0.02	2.9155E-04	0.03
Cost group 4 < £10K	19.653E-04	1.19	2.2819E-04	0.23	2.3537E-04	0.24
Cost group 5 < £100K	13.003E-04	11.94	2.2819E-04	2.28	2.2776E-04	2.28
Cost group 6 < £1M	11.941E-04	119.4	2.2819E-04	22.8	2.2654E-04	22.7
Cost group 7 < £10M	11.941E-04	1,194	2.2819E-04	228	2.2654E-04	227
Cost group 8 < £100M	11.941E-04	11,941	2.2819E-04	2,280	2.2654E-04	2,270
Cost group 9 < £1B	11.941E-04	119,410	2.2819E-04	22,800	2.2654E-04	22,700
Cost group 10 < £10B	11.941E-04	1.194M	2.2819E-04	228,000	2.2654E-04	227,000

Table 8.21 – Risk distribution profile

Relevant computer run results can be examined in the software files included in the CD/DVD; see folder titled Ops X Operations/ Ops X Belief/ BBN files.

Although Table 8.21 provided risk values, the study could not form a judgment on the significance of the risk value as an Accountable Manager (AM) would form. An AM/CEO would have a wider view of all other financial information for the company, i.e. the business objectives, costs, profits and liabilities etc. Thus they would be able to weigh this risk of CAW error against all other risks that an AM is required to cover.

For instance, under regulation, an operator is required to insure his aircraft against passenger, flight crew and third party liabilities in the event of a catastrophic accident. Human error might trigger the consequences that would end up as a catastrophe, but from the evidence available, most human errors in CAW contribute only a marginal risk as demonstrated here. The larger risks that an operator is required to cover under regulation would come from pilot error, equipment unreliability, airfield and ATC management, bad weather, terrorist activities and acts of God.

For a Boeing 757 the insured value for third party liabilities is of the order of £300M, and it does not include the cost of replacing the lost aircraft. The risk value that the model returns at the cost group equivalent to £300M, i.e. Cost Group 9, is £22,700.

Thus if the estimated Costs assumed for the trial were to be taken as real cost of consequences, then it is possible to say that for this operator, the risk contribution due to human error in CAW processes was only £22,700 per £100M when the CEO/AM was covering a liability for third party claims of at least £300M. This study considers that this a reasonable risk to take.

In contrast, if short period experience alone was taken into consideration, i.e. 34,338 sectors only, then the risk level increases to £119,410 per £100M per flight based past experience to that point in time. It is nearly a 5 fold increase, which a CEO might consider unreasonable.

8.19 NETICA - Handling of parameters for which data not available

It is necessary to explain the reasons for the model returning prior probabilities for certain states of nature within the nodes, even when evidence, albeit they are limited, has indicated that those states of nature did not occur.

There are two reasons for this. One is the computing technique that handles zero evidence, and the other is a more realistic issue in probability concepts relating to the probability of events happening due to unknowns. This latter cannot be ignored simply on account of the fact that there was no data for the relevant states of nature. As long as they have been identified as possible outcomes, they would have a probability of occurrence though not known.

NETICA handles this issue at the Conditional Probability Table (CPT) for the relevant node, which has been integrated into its software. The CPT collects data for various combinations of parent nodes' states of nature and those states defined for the child node. A specimen CPT is given in Table 8.22 that summarises the input data according to the combination of events.

Takeoff (Parent Node)	Flight and Consequences (Child Node)						
	No Error	Flt completed error CF	In flight shut down, Flight completed	Incident RTB	Incident Flight Diverted	Non fatal accident	Fatal accident
No Error	34239	0	0	0	0	0	0
Error	0	98	0	1	0	0	0

Table 8.22 - Input data counts

It can be seen that data was available for only 3 of the 14 cell-combinations in this matrix. In order to handle the unknown, the program modifies the CPT by inserting

one event in each blank cell and balances this action by adding one event in each cell containing data. The outcome is as shown in Table 8.23.

Takeoff	Flight and Consequences						
	No Error	Flight completed error CF	In flight shut down, Flight completed	Incident RTB	Incident Flight Diverted	Non fatal accident	Fatal accident
No Error	34239+1	+1	+1	+1	+1	+1	+1
Error	+1	98+1	+1	1+1	+1	+1	+1

Table 8.23 - Data modified i.e. normalized

Following this modification, the total experience is taken as 34352 events (i.e. 34246 + 106) as at Table 8.24 whereas the pre-modified experience was 34338 events (Table 8.22). This is the standard NETICA practice, as per NETICA User Guide's Section 10.2[90].

Takeoff	Flight and Consequences
No Error	34246
Error	106

Table 8.24 - Data modified – New experience

Simple probabilities are then calculated on the total experience in which the summation of each line's probability values should add up to 1 or 100% (Table 8.2). Note that there are no zero probability values in those cells where actual data for the trial period turned out to be zero.

Takeoff	Flight and Consequences						
	No Error	Flt completed error CF	In flight shut down, Flight completed	Incident RTB	Incident Flight Diverted	Non fatal accident	Fatal accident
No Error	0.999825	2.92005E-05	2.92005E-05	2.92005E-05	2.92005E-05	2.92005E-05	2.92005E-05
Error	0.00943396	0.933962	0.00943396	0.0188679	0.00943396	0.00943396	0.00943396

Table 8.25 - Conditional probabilities based on modified data – new experience

Utilizing these simple probabilities of arising, as well as other upstream conditions defined by the BBN, NETICA program then calculates the conditional probabilities for

each of the states of nature (consequences) at this node. Results were already given in Table 8.19, Column 2, reproduced at Table 8.26. These values are rounded off and pictorially presented in the BBN, but the actual high resolution values could be read off from hidden files in NETICA software embedded deep within the CAW Risk Model. An example is tabulated below, Table 8.26 and Figure 8.17.

Category of consequence	Validation trial
No of lines/ sectors	34338
No error	0.99742
Flight completed- error carried	0.002300
Incidence- flight diverted	5.21E-05
Incidence RTB	7.50E-05
In flight shut down	5.21E-05
Major accident	5.21E-05
Fatal accident	5.21E-05

Table 8.26 – Distribution profile of Flight Consequences

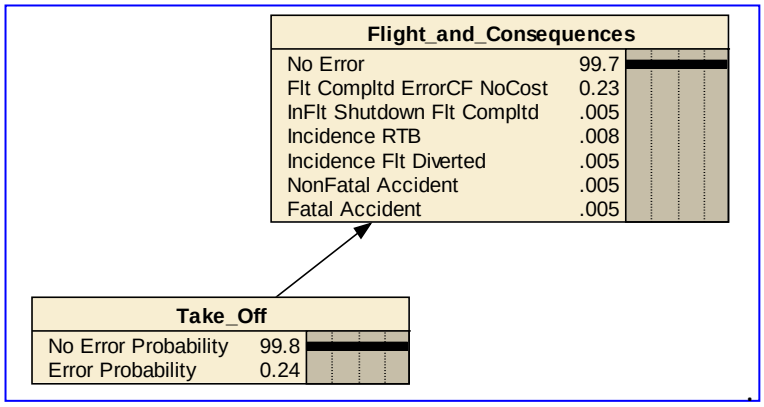


Figure 8.17 – Mapping conditional probabilities to BBN nodes

This study has researched the theoretical justification and mathematical basis for this technique, where a small equal amount is added to each cell in order to learn Dirichlet priors as the technique is called. It is rooted in research by Spiegelhalter et al (1993) Section 4.1[89] which explains how to handle situations when conditional probabilities themselves were unknown quantities. Although the verification of Spiegelhalter's work was outside the remit of this study, there was confirmation of its integrity by Norsys Software Corporation (in a letter to the researcher) which utilises the theory in their commercial software that has been widely accepted throughout the world. The results obtained during the exercise to derive global safety level profile through simulation have in fact provided an alternative form of verification of the technique.

There are further qualitative justifications for the use of this technique. Addition of one event to each cell of the CPT might appear to give a pessimistic view of the performance of the organization, because the experiences taken into account in the calculation are more numerous than those actually encountered. But in reality what it does is to make the acknowledgment that all those identified combinations are possible. In the absence of any other data an estimate is made that the probability of that combination occurring is very small. This is better than stating that the combination could not occur according to one's experience, because if the possibility exists then a finite probability exists no matter how small it is.

This probability can neither be negative nor zero. If zero value was left in a cell because no events were actually experienced, then it would return a zero probability. An event that may be possible but not yet occurred is not the same as a zero probability. A zero probability means that the event is an impossibility, which is not true, if the event has been already defined as in the model.

If not zero, the cell entry would have to be a one, because an event cannot be a fraction. Therefore, it makes sense for the program to count one event against each cell in the "Counts Mode" as part of initializing process for the program.

The outcome of this computing technique is that even if the event had not actually happened, the output would show a probability of the event occurring, which is exactly as it would be the reality in nature.

On equal distribution of probabilities across those states of nature where data is not available, this too has merit. If there is no knowledge about their behavior, then there is no other option than accepting that any one of the possible events is equally likely to occur.

The magnitude of the probability is open to debate, and therefore its accuracy and the question if this representation is fair. The accuracy depends on the actual number of sectors flown. If the number of data lines (i.e. sectors flown) is small, then the probability of the event occurring is shown as high, because the simple probability values stated in the CPT comes from the formula:

No of events in the error combination /Total number of errors experienced ……. 8.1

This is in fact correct as an argument even though the numeric value has been slightly modified. It may be possible to reconcile with the result that it indicates the level of uncertainty as a probability but not as an exact absolute truth. To give an analogy,

given a meter has been defined, one kilometer has 1,000 meters, which is absolute truth, whereas degree of uncertainty as a probability is relative and depends on what is known and what is not known. It is not possible to define what is not known and therefore an assumption has to be made.

If the sample is small then less is known about the behavior of the organization, and there is less knowledge and experience with conditions under which incidents could occur. Therefore it is quite feasible and reasonable that there is wide scatter of the probability of something happening, compared to that from another who has flown a several million more sectors and its reliability has been well proven. This is because the event would happen in a defended system, and the risk has a dependency on the experience as well as defenses.

Quite simply, insufficient knowledge of an operation may lead to estimating the likelihood of a severe event occurring as high. At best, if one of several consequences is possible but there was no previous experience of their distribution (at the specific operator) then the fairest estimate is an equal likelihood of any one of them occurring. The equal distribution of probabilities will reduce the numerical value of any one of them as the total uncertainty is spread out over several possibilities. In contrast, if the number of sectors flown is large, then the calculated probability will be proportionately smaller.

This situation can be best demonstrated by referring back to the Dirichlet's probability distribution curves given in Chapter Five, Figure 5.14. If less is known about the organization, then the distribution of unknowns at higher values will have a flat spread (graph at lower-left corner). If the operator has greater experience, say, several millions of sectors flown and a lot is known about the operator, say, they are consistently safe, then the peak of the graph rises rapidly (as No-Error flights are recorded); in the process, the rapidly increasing peak value, pulls down the probability values towards the tail end of the probability distribution curve (see graph at the lower-right hand corner). This is because the total probability would add up to 100%; if the peak rises, the tail end should dip provided that the operator is dynamically stable. In real life, the curve would be highly skewed to the left (No-Error) and then drop rapidly giving a tail that is asymptotic to infinity. There is not enough data available to the research study to create such a distribution profile. In any event, each operator should be considered on its own merit.

There are two other techniques for handling states for which data is not available.

- **Technique 1** is to truncate the model by eliminating those nodes for which data not available. Introduce them later when new information is available. Academically, or as a research study it has merit, but not as a practical tool in industry. If the possibility of a state exists, then it could occur any time, and the model must make provision for it in the model. Operators must have full visibility of all possible "states", if not they would not be able to correctly allocate the most relevant causal factor. Anything "not seen" may be taken as it "does not exist". Furthermore, a later addition of new "states" would change the structure of the model and probabilities. The end result after modification could have a significant step change that would be difficult to manage if the concept has been used for assessing risk over a long period. In contrast, a small change would have no impact as risk values usually change with updating, and the organization is used to tolerate small changes.

- **Technique 2 is to e**liminate those combinations that are considered impossible. In this generic model the number of combinations is so large, running into almost 3M, it is impossible or impractical to undertake this entire task manually. As it would be improper to eliminate some and leave others, all combinations were retained regardless of the fact if they are possible or not. In fact further investigation into this issue revealed that the Bayesian research community has already recognized the difficulty of truncating unlikely combinations from large number of combinations. Other computer techniques have to be used for their development, which is still at research stage according to enquiries made during this study.

The decision to leave all combinations intact has other justifications. For instance, the range of events and causal factors that were included in the model was not exhaustive. Only those parameters that were either obvious, brought to our notice by expert LAEs, or suggested through other research papers have been included. It is not a fully surveyed listing. There may be many other events and causal factors that deserved mention as possibilities. Similarly the number of nodes is also not exhaustive. The model may need other nodes to represent the full CAW process as an ID. Since this is a generic model, the study was not too concerned about obtaining a definitive list of nodes and causal factors, but as many as possible to maximise scope and to demonstrate what the models capabilities are.

Given these other possibilities and limitations of knowledge, the study accepted the argument that even if an aircraft had gone through all the critical nodes as error free,

there could still be other conditions unaccounted for, which could contribute to human error that would affect risk. There have been instants when an aircraft has had a dormant problem or an error, it has gone through final checks at critical nodes and cleared as safe to fly, yet the error resurfaced during flight resulting with an incident. Therefore, clearance of an aircraft as safe by CAW process has a legal validity that it is airworthy, but still it might not give a guarantee that the aircraft will be 100% safe and airworthy. An infinitesimally small probability of risk could still remain. Ironically, it is in fact the events that occur at those infinitesimally small scale of probability or limits of imagination that cause accidents, and not the obviously glaring hazards.

Accordingly, this study adopted the technique that no combination would be eliminated, just because the process seemed to provide adequate safety, or because some combinations were unlikely or appeared to be not relevant. In accident, relevancy or the lack of sufficient safeguards, checks and balances emerges during the investigations after an accident. The study moved away from the idea that experts knew it all, and erred towards uncertainty and incompleteness of information; this was the most rational and common sense posture to adopt. Thus no combinations were truncated on account of apparent irrelevancy. The result from simulation proved that retention of all combinations to account for unknowns is justified.

8.20 Reliability of validation trial results

The operator had raised a query on the reliability of the results and applicable confidence levels. It has already been shown that the number of sectors flown has a significant impact on the probability values output by the model.

In response it should be stated that the validation trial was not a sampling exercise from which predictions on the whole population would be made. Although the trial was limited to only a proportion of flying that the operator had undertaken since the licensing of this AOC Holder, the trial made use of all the flying that was done during a period when systematic error data recording had been undertaken. That means the entire population of available data was used in the trial.

The objective was to test the possibility of using the result as a starting point, i.e. to set a reference line, and then to continue with the building up of a full error data history for the fleet. The reference line would certainly be affected by the number of sectors flown. Thus, it was envisaged that new operational data would be added to the database, and simultaneously, through continual updating, the model would calculate new probability values enabling change of risk level to be determined. This

technique could be used for monitoring the safety performance of the operator and trends.

That said, statistical reliability and confidence levels become relevant if the result, e.g. the calculated risk level, was to be used as a bench mark for comparing one operator's safety performance with another operator's or with a global or national standard. In that case, the population size, i.e. the number of sectors flown, would have a major impact on the reliability of the result. If one operator has flown million sectors in one year, and the other has flown 30,000 sectors, then the result from the larger operator becomes more reliable than that from the smaller operator, given other conditions remain on par. Reliability of the test results could be quantified by calculating statistical confidence limits to the required level of confidence.

Table 8.27- Fleet Maintenance Operation - Errors observed for period Jan 08 – Feb 10

Date	ID	AC Type	AC ID	Nature of Error	AMO Location
1 Feb 08	41	Type_A2	Reg_6	Refuel valve fails to open due faulty relay fitted.	L3
13 Dec 08	19	Type_A2	Reg_7	Loose articles (fasteners) in pneumatic coupling	L1
25 Dec 08	23	Type_A2	Reg_9	Loose article (Oil can) left in engine pylon	L1
4 Feb 09	23a	Type_A2	Reg_9	Loose article (Oil can) found in engine pylon during C Check.	Dormant
28 Feb 09	27	Type_A2	Reg_9	EGPWS spurious warnings led to radar altimeter transmitter/receiver loose connectors	MRO1
1 Mar 09	27	Type_A2	Reg_9	EGPWS spurious warnings misdiagnosis	MRO1
3 Mar 09	27	Type_A2	Reg_9	EGPWS spurious warnings misdiagnosis	L2 Base
4 Mar 09	27	Type_A2	Reg_9	EGPWS spurious warnings misdiagnosis	L4
5 Mar 09	27	Type_A2	Reg_9	EGPWS spurious warnings misdiagnosis	L1
7 Mar 09	27	Type_A2	Reg_9	EGPWS spurious warnings misdiagnosis	L1
11 Mar 09	27	Type_A2	Reg_9	EGPWS spurious warnings misdiagnosis	L10
15 Mar 09	27	Type_A2	Reg_9	EGPWS spurious warnings	L2 Base
30 Mar 09	4	Type_A2	Reg_6	Inoperative cargo deck rollers	L2 Base
3 Apr 09	4d	Type_A2	Reg_6	Inoperative cargo deck rollers	L2 Base
21 Apr 09	35	Type_A2	Reg_16	Post C Check, loss of Oxygen accumulator pressure	MRO1
30 May 09	37	Type_A2	Reg_10	Transfer of No-Go Item to ADD	L1
24 Jun 09	39	Type_A2	Reg_8	Missing Splice	Prev Owner
3 Jul 09	40	Type_A2	Reg_14	Engineer forgot to deactivate battery charger	L46
3 Jul 09	40a	Type_A2	Reg_14	Active battery charger – dormant error	Dormant
3 Jul 09	40b	Type_A2	Reg_14	Active battery charger – dormant error	Dormant
3 Jul 09	40c	Type_A2	Reg_14	Active battery charger – dormant error	L1
2 Aug 09	43	Type_A2	Reg_8	Circuit breakers left pulled post maintenance	L1
2 Aug 09	44	Type_A2	Reg_22	Incorrect robbing procedures and tech log certification	L1
10 Aug 09	47	Type_A2	Reg_19	APU oil empty due to incorrectly installed filler cap	L1
24 Aug 09	48	Type_A2	Reg_12	Incorrect Decal markings at fuel drip stick locations on both wings	L2 Base
26 Aug 09	51	Type_A2	Reg_1	UC gear pin stowage missing	L1
28 Aug 09	55	Type_A2	Reg_3	Red "remove before flight" ribbon hanging from flaps	L1
31 Aug 09	50	Type_A2	Reg_17	MEL not followed, initially, to clear status message (“R ELEV PCU”)	L1
31 Aug 09	53	Type_A2	Reg_19	Cabin door opened without deactivating power assist	L1
9 Sep 09	46	Type_A2	Reg_15	Thrust reverser Incorrect sensor adjustment, rigging and tech log certification.	L1

Date	ID	AC Type	AC ID	Nature of Error	AMO Location
11 Sep 09	11	Type_A1	Reg_24	3-day over-run of fuel sump draining	MRO2
15 Sep 09	1	Type_A1	Reg_23	Structure fouling	Pt 21 POA
15 Sep 09	1b	Type_A1	Reg_23	Structure fouling	Pt21 POA
15 Sep 09	57	Type_A1	Reg_23	Engineer slipped, sprained ankle and damaged skin of the outboard aileron	L2 Base
24 Sep 09	5	Type_A2	Reg_7	Reported ac light on rotation	Dormant
24 Sep 09	5e	Type_A2	Reg_7	Reported ac light on rotation	L1
30 Sep 09	59	Type_A2	Reg_14	Damage to spinner assembly done as a result of investigating OSIC	L1
6 Oct 09	6	Type_A2	Reg_14	Improper robbing procedure	L2 Base
6 Oct 09	9	Type_A2	Reg_5	Faulty wiring of fuel pump	MRO1
6 Oct 09	60	Type_A2	Reg_20	Tech log open defect	Flt Crew
17 Oct 09	9i	Type_A2	Reg_16	Faulty wiring of fuel pump	Unknown
27 Oct 09	61	Type_A2	Reg_5	CB information on MEL regarding cargo aft fan incorrect	L2 Base
2 Nov 09	2	Type_A2	Reg_19	Overdue Service Check	L3
2 Nov 09	8	Type_A2	Reg_21	Failed to record fuel state on Tech Log after defueling for maintenance work	L1
3 Nov 09	9d	Type_A2	Reg_10	Faulty wiring of fuel pump	
3 Nov 09	9f	Type_A2	Reg_11	Faulty wiring of fuel pump	
13 Nov 09	63	Type_A2	Reg_9	Rumbling noise from nose wheel	L1
12 Dec 09	9k	Type_A2	Reg_18	Faulty wiring of fuel pump	
17 Dec 09	9c	Type_A2	Reg_8	Faulty wiring of fuel pump	
27 Dec 09	9g	Type_A2	Reg_14	Faulty wiring of fuel pump	
27 Dec 09	9j	Type_A2	Reg_17	Faulty wiring of fuel pump	
28 Dec 09	9h	Type_A2	Reg_15	Faulty wiring of fuel pump	
1 Jan 10	64	Type_A1	Reg_24	Aircraft slipped off axle jack during wheel change.	L1
15 Jan 10	3	Type_A3	Reg_25	Incomplete maintenance due to distraction	L1
16 Jan 10	16	Type_A2	Reg_5	Smoldering fire in 2 cable bundles and burnt wires.	Pt 21 POA
17 Jan 10	9b	Type_A2	Reg_6	Faulty wiring of fuel pump	NK
22 Jan 10	13	Type_A2	Reg_12	Burnt and separated wiring in a loom	Pt 21 POA
11 Feb 10	17	Type_A2	Reg_15	Insufficient bleed of hydraulic system after leg replacement	L1

Table 8.27- Fleet Maintenance Operation - Errors observed for period Jan 08 – Feb 10

Table 8.28 - Findings from Audits and Regulator Oversights

Date	Relevance	AC ID	Nature of Error	AMO Location
16-Jun-08	General organization	General organization	CAME Procedure 9.2.3 should include an explanation of required inspection	L2 Base
20-Aug-08	Type-A2	Reg-21	Spoiler removal NRC card does not meet DAEP10 requirements for independent inspections	MRO3
20-Aug-08	Type-A2	Reg-21	C Check tally sheet missed out control entries for removal and refitting of access panels	MRO3
20-Aug-08	Type-A2	Reg-21	Job Cards 72 and 73 had no findings recorded; it should have C-EAT Ac Type A2-51-43-06	MRO3
20-Aug-08	Type-A2	Reg-21	3-task cards among control documents had no card reference numbers, and not listed in the tally sheet. They were unrelated to aircraft worked on at this location	MRO3
12-Sep-08	General organization	General organization	Description of facilities 1.8.4.7 for BFS station incorrect. Accommodation was changed in Mar 08. i.e. documents out of date.	L23
07-May-09	General organization	General organization	Laptop is the only accessible means to digitized data. If laptop failed there was no other method for access to maintenance data	L10
07-May-09	General organization	General organization	Tech Log page 83119 has no aircraft registration details pre-printed as per DAEP 6 procedures, pg 4	L10
27-May-09	General organization	General organization	Privilege of ARC extension not detailed in personal authorization documents	L2 Base
15-Mar-10	Type-A2	Reg-6	Contractor non compliant with MA708b; unable to demonstrate they were in full control of the management of task cards vide MA708b	MRO1
11-Jan-08	Type-A2	Reg-21	Contractor cleared ADD entry whilst not sanctioned by inter-facing contract to do so.	L2 Base
11-Jan-08	Type-A2	Reg-21	Aircraft maintenance manual copies were out of date.	L2 Base
11-Jan-08	Type-A2	Reg-9	Company had no contract with the 3rd party contractor who repaired this aircraft	L2 Base
30-Jan-08	General organization	General organization	Calibration certificates unrecorded on TRAX causing equipment status unreliable	L2 Base
30-Jan-08	General organization	General organization	Bonded store insecure enabling access by unauthorized personnel	L2 Base
30-Jan-08	General organization	General organization	Accessibility to airworthiness data unsatisfactory 50% of the time	L2 Base
30-Jan-08	General organization	General organization	Line PC had no access to EMOS or Safety Net	L2 Base
30-Jan-08	General organization	General organization	Insufficient access to maintenance data. Inadequate number of PC access points.	L2 Base
31-Mar-08	General organization	General organization	Faulty audit report raised because QA used an electronic document standard that had not been updated. Paper and electronic forms were inconsistent. Change Management has been defaulted for not having the same standard.	L2 Base
31-Mar-08	General organization	General organization	Faulty standard used by QA. Reported finding invalid. Maintenance certificate erratic as ac released under misquoted authority. Aircraft should not have been released without rectifying the defect.	L2 Base
29-Apr-08	General organization	General organization	For 2 engineers, either no file or no training certificate on file.	L2 Base
29-Apr-08	General organization	General organization	Appraisal certificate missing for engineer.	L2 Base

Table 8.28 - Findings from Audits and Regulator Oversights

Date	Relevance	AC ID	Nature of Error	AMO Location
06-May-08	General organization	General organization	TRAX data on the disposition of major assets were incorrect. Engine S/N 30070 allocated to an aircraft whereas it was in fact off wing and at POA on major overhaul. 13 engines were allocated wrongly on TRAX.	L3
28-May-08	General organization	General organization	L15, Line Maintenance, No tooling inventory available.	L15
28-May-08	General organization	General organization	Equipment calibration records were not properly managed.	L15
28-May-08	General organization	General organization	No stockholding sheet for shelf items, even though life control items were being controlled by L2 Base logistic.	L15
09-Jun-08	General organization	General organization	Training staff not fully conversant with company procedures and processes. Trainers needed training.	L16
09-Jun-08	Type-A2	Reg-20	Details of work required, authority and references were not stated in the Tech Log (as it should be) following authorization to repair a defect was given by L2 Base maintenance control centre	L16
09-Jun-08	Type-A2	Reg-20	AC released without providing references to an approved repair scheme or procedure.	L16
10-Jun-08	General organization	General organization	Engineer's file not updated with his HF training certificate.	L6
16-Jun-08	General organization	General organization	No shift handover diary maintained.	L1
17-Jun-08	General organization	General organization	No handover log maintained.	L1
02-Jul-08	Type-A2	Reg-15	Part M AO CAW records unsatisfactory. Irregular recording of aircraft hours.	L3
02-Jul-08	Type-A2	Reg-19	Part M AO CAW records unsatisfactory. Irregular recording of aircraft hours and engine installation not signed for.	L3
11-Jul-08	General organization	General organization	No MCC training certificates held for MOC staff.	L1
22-Jul-08	General organization	General organization	Nitrogen cylinder due calibration was not replaced by management.	L5
22-Jul-08	General organization	General organization	Contractor had not supplied an up to date listing of technical manuals to Line Station at L5	L5
28-Jul-08	General organization	General organization	Inadequate cargo deck rollers inspection frequency, to be increased from 1C check to 3A Check.	L2 Base
30-Jul-08	General organization	General organization	L15 library failed to show a receipt for the return of a Type 2 aircraft MEL document. Investigation revealed that no MEL was ever sent to L15.	L15
30-Jul-08	General organization	General organization	Flight Ops library unable to reassure about fuel quantity measuring stick data due to the absence of an updated document. Different document to an old revision state is available, but no one sure what the latest standard was.	L2 Base
16-Sep-08	General organization	General organization	Gas cylinder storage and husbandry unsatisfactory.	MRO1
16-Sep-08	General organization	General organization	Manual 323 CMM Fire Overheat Detector Rev 7 had not been incorporated	MRO1
16-Sep-08	General organization	General organization	DAEP temporary revision folder was missing and unaccounted for	MRO1
09-Dec 08	General organization	General organization	No minutes of meetings between Accountable Manager and Heads of Dept maintained, meaning no policy decisions are recorded.	L33

Date	Relevance	AC ID	Nature of Error	AMO Location
11-Jun-09	General organization	General organization	Maintenance Control Centre at L1 had no visibility of contracts that parent operator maintained with other 3rd party contractors at outstations.	L1
13-Jun-09	General organization	General organization	Check Pack "A" incomplete.	L1
13-Jun-09	General organization	General organization	No Tech Log entry made at the commencement of A-Check. Error on part of the Supervisor, but primarily attributed to training program differences at L1	L1
13-Jun-09	General organization	General organization	A-Check supervisor was unaware of company procedure due to different training standards.	L1
13-Jun-09	General organization	General organization	Task card requires changing from Mechanic to Inspector annotation following changes procedures. Cards should be updated	L1
13-Jun-09	General organization	General organization	Delay in A-Check caused by lack of printing equipment for tech documents. This is not strictly an error but an admin or management shortfall.	L1
15-Jun-09	General organization	General organization	L1 contractor has a backlog of untrained staff due to lack of Trainers	L1
15-Jun-09	General organization	General organization	Large backlog of QA observed Non-Conformances awaiting AO's approval	L1
08-Jul-09	General organization	General organization	Engines with misaligned spinner caps still received by POA for engines, despite a previous audit report highlighted this problem. Problem was engineers not following AMM procedures.	L2 Base
17-Sep-09	General organization	General organization	L2 Base MOC under-manned and after 8-months still no improvements to manning situation. No recruiting in the offing.	L2 Base
17-Sep-09	General organization	General organization	Access to CAME and DAEP restricted due to lack of proper electronic links to the server.	L2 Base
28-Oct-09	General organization	General organization	MOE manpower plan out of date. Not updated.	MRO1
28-Oct-09	General organization	General organization	MOE revision status page not signed.	MRO1
28-Oct-09	General organization	General organization	MRO1 does not record ADD Ref Num block when clearing ADDs, making it difficult to track and manage ADD entries on TRAX system. TRAX system expects to use these entries.	MRO1
28-Oct-09	General organization	General organization	MRO1 safety data spread sheet is widely out of date, and needs updating.	MRO1
28-Oct-09	General organization	General organization	Incident Report form, No Entry annotated to protect identity or anonymity.	MRO1
28-Oct-09	General organization	General organization	HF training out of date for one engineer.	MRO1
28-Oct-09	General organization	General organization	No management traceability of engineers reading Safety Notices placed on the notice board. Need a better traceability system.	MRO1
28-Oct-09	General organization	General organization	Engineering Quality Manual amended to revised status, but the fact was not recorded in the amendment page.	MRO1
30-Oct-09	Type-A2	Reg-14	Poor husbandry. Off ac equipment unlabeled, not segregated and unprotected from pollution. Lacking in technical discipline	MRO1
27-Nov-09	General organization	General organization	Third party contract has not been updated	L75
20-Jan-10	General organization	General organization	Inventory of tooling and parts 8-months out of date	L10
20-Jan-10	General organization	General organization	Management of amendments to tech documents unsatisfactory. Amendments have not been incorporated in a timely fashion, making documents unreliable	L10

Table 8.28 - Findings from Audits and Regulator Oversight

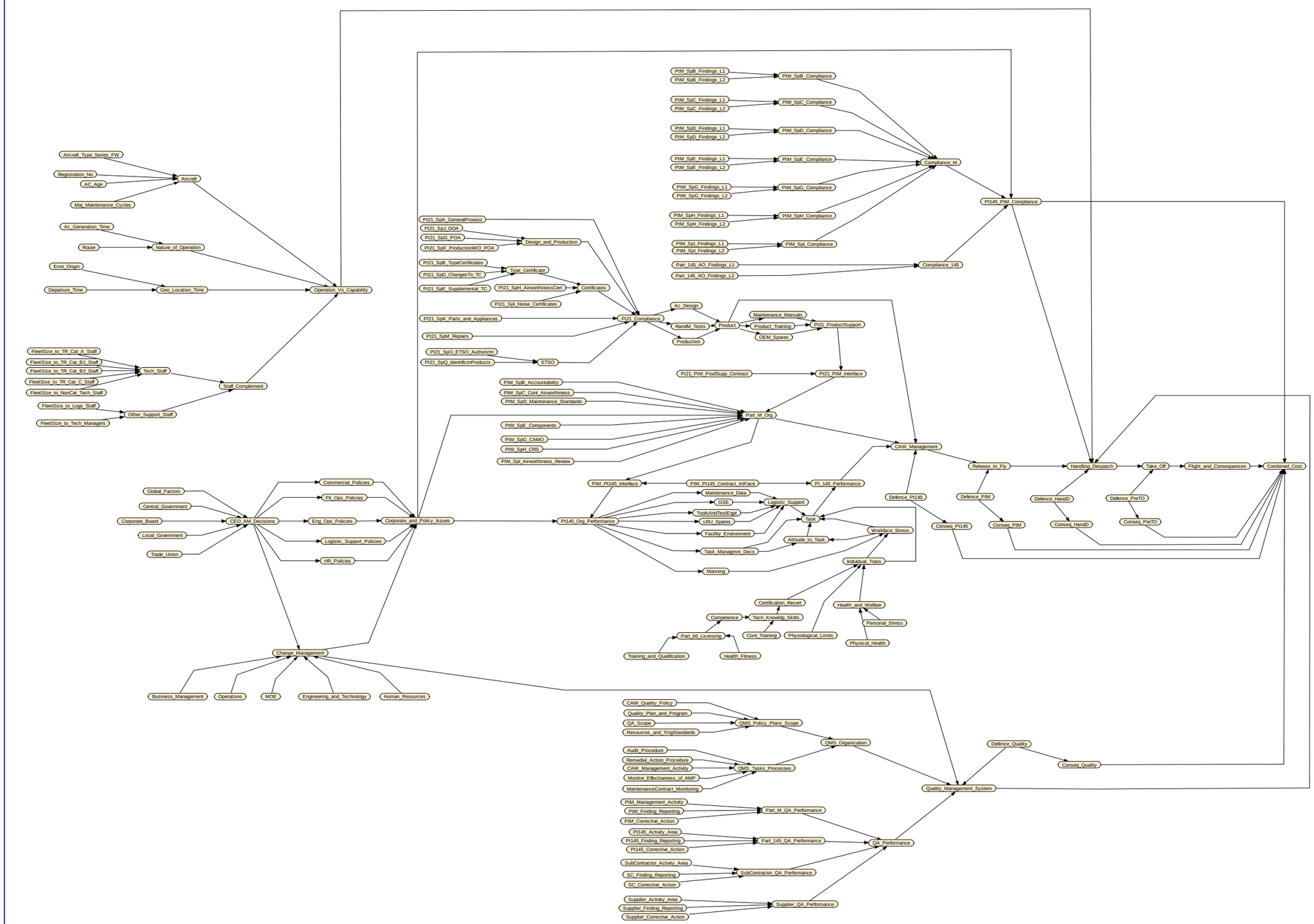


Figure 8.18 – Generic CAW Risk model modified for Operator X used in validation trial

Intentionally Blank

Chapter Nine

Discussion – Model application

9.1 Introduction

This chapter takes an overview of the CAW Risk Model's potential for application in air transport industry as a general strategic level risk assessment tool for use by high level managers.

During the advanced stages of this research, participating operators and the Regulator raised a number of specific questions in order for them to assess the practicability of the model within civil aviation industry.

- Could this model be adopted as part of an operator's SMS?
- Would it be suitable for publication in UK CAA SMS guidance material?
- Bearing in mind the significant man-hours associated with populating this model would the industry be willing to adopt this?
- What would be the cost benefit to industry?
- Could CAA establish a baseline risk acceptance level using this model?
- How should the CAA create equality of an acceptable level of risk across industry?
- How do you see the CAA establishing acceptable levels of trend deviation?
- Would it be possible to set league tables as a consequence, say, categorized as gold, silver, bronze standards?
- What is the risk to the CAA of "backing off" from the current oversight regime?

The Chapter first considers if the model met its intended industrial needs, i.e. as a supporting tool in the application of RBO concept and in SMS. The responses to the questions follow as a discussion, where the differences between the desired objectives and what is practical in an industrial environment are reconciled.

Some of the information given here are personal opinions of the individual airworthiness experts who participated in the program. Nevertheless, they were a part of the research and could be considered as valid expert opinions.

9.2 Regulatory role – Model supporting RBO concept

In RBO application the model meets the desirable criteria for a quantitative risk model as visualized in Philip Hampton Report[13], see Table 9.1. The following sections qualify them.

9.2.1 Open to scrutiny. The BBN concept is well documented and proven in other areas of application. Software programs used in the core of the model for calculating conditional probabilities are well known and commercially available. Therefore the underpinning theories and technical logic are open to full scrutiny.

9.2.2 Past performance and potential risk. The database, on which the model calculates, represents the performance of the organization up to that point in time. It uses past data to estimate current potential risk. Where error data is not available, e.g. in a newly established organization, it may be possible to simulate data based on beliefs.

Criteria (Source – PH Report)	BBN
Open to scrutiny	Yes
Balanced to include past performance and future potential risk	Yes
Use all good quality data	Yes
Implemented uniformly and impartially	Yes
Express simply, preferably mathematically	Yes
Dynamic and not static	Yes
Carried through to funding decisions	Yes
Include an element of random inspection	Yes
Incorporate deterrent effect	Yes

Table 9.1 - Meeting desirable criteria for a risk model

9.2.3 Good quality data. Obviously, calculations based on simulations would not be accurate as those based on hard evidence. All good quality data, i.e. hard evidence, would be used first and the least reliable data last. Poor quality data would be gradually faded out as more and more good quality, new information is accumulated.

9.2.4 Calculates current risk. Once the model calculates current risk as determined by the historical data collected to that point, it is possible to ascertain the trend by regular updating. Management could be alerted to potential increases of risk level and by identifying hazards that cause increasing risk.

9.2.5 Uniform and impartial implementation. Since the risk assessment is based on a statistical calculation to a formula and is structured, the methodology remains the same regardless of who would use the model; personal opinion does not come into it. However the initial handling of the event, if it was to be reported or not, or to be investigated, and its categorization, all these could be affected by an individual or by local safety culture. Rules for reporting and categorization of data could be written in order to reduce this personal bias and to make the process as neutral as possible.

9.2.6 Mathematical expression. The output is expressed mathematically, and simply in terms of a probability of an error occurring, the probability of consequences resulting from the error and the probability of the cost related to that error.

9.2.7 Dynamic process. It was explained that the risk assessment process is a live, on-going process as data are continually accumulated and calculation updated. Thus the process is dynamic. The latest state of play can be read off at any time by managers.

9.2.8 Results carried through to funding decisions. It is the management who would decide if the output from the model would be carried through to funding decisions. The model provides the supporting information: i.e. the risk level, trends, points in the process where significant causal factor concentrations exist and the sensitivity of risk to certain causal factors. After that, it is up to the management to make the best use of this information in their funding decisions.

9.2.9 Random inspections/ audits. Issues concerning either random inspections or deterrent effects are concerned with the application of the model to monitor regulatory compliance. For example, if there were to be any relaxation of the oversight regime on account of RBO concept and the degree of control that the Regulator might wish to retain in order to enforcement the law. These are management and administrative activities. The model is only a tool to enable both the operator and the Regulator to assess the risk.

9.2.10 Performance indicators. Through sensitivity analysis it is possible to identify specific nodes in the process network, which are critical to the safe operation. If these could be monitored, then they could become relevant performance indicators. From a problem solving viewpoint, indicators based on sensitivity analysis may be better than those currently used, i.e. number of MOR raised or the number of accidents or incidents industry-wide. This issue is further discussed in Section 9.9.

9.3 SMS implementation – Model's support role

The potential use of the risk model as a supporting tool in a safety management system answers the first question posed by UK Regulator, i.e. if it should be considered for adoption as part of the SMS. It was already stated that the ICAO mandate on SMS has revived authorities' interest in and need for a reliable risk assessment methodology that provides a quantitative output. This model meets that need. This section explores how the risk model fits into a safety management system.

ICAO Doc 9859 SMM states that a SMS should have the following elements, namely:

- Policy for and the organization of SMS.
- Methodology and process for safety risk management and its implementation.
- Continuing safety assurance process.
- Safety awareness and promotion program.

CAW Risk Model satisfies two of the elements, i.e. it provides a methodology and a process for safety risk management as well as a continuing safety assurance process.

Process (Source – SMM ICAO Doc 9859 Ch 8)	Subjective judgment – expert opinion	BBN
Hazard identification	Identifies new hazards	Works with previously identified hazards
Risk assessment	Susceptible to self-protection as well as business pressures	Neutral
Probability of the hazard precipitating an unsafe event given optimum conditions	Informed individual judgment – wide margin of error	Data driven
Severity of consequences	Informed individual judgment – wide margin of error	Data driven
Rate of exposure to unsafe conditions, i.e. conditionality	Informed individual judgment – wide margin of error	Data driven
Risk assessment/ estimation	Inexact – informed judgment	More exact
Acceptability of risk	Subjective judgment but standards may vary with business pressures	Relative to previously set threshold
Risk mitigation	Individual personal decision on how to mitigate, then subjective judgment if it works	prioritizes critical causal factors + validate effectiveness of mitigation
Performance indicators	Set subjective standards	Data driven, yields KPI

Table 9.2 - Model comparison – Traditional vs BBN

Table 9.2 compares the relative strengths and limitations of the risk model with traditional subjective methods, using ICAO Doc 9859 statement on the capabilities of a satisfactory SMS; it must be capable of: hazard identification, risk assessment, output

risk value as a tangible measure, deciding the acceptability of the risk, risk mitigation, and setting new performance indicators.

On hazard identification, the traditional system works better because a human could identify new hazards whereas a model cannot do it unless it is linked with sensors and pre-programmed. Unfortunately, unknown conditions cannot be modelled, i.e. the BBN model could work with previously identified or predicted as feasible situations.

In all other respects the CAW Risk Model is far superior to the traditional methods.

Risk assessment is based upon three factors coming together: the probability of a hazard precipitating to cause an unsafe event, the severity of consequences and finally the rate of exposure to unsafe conditions. In the traditional system all these 3 factors are based on expert opinion, whereas in the BBN model, they are data driven. Expert opinion may be bias, conservative and may have an element of self preservation against the unknowns, whereas the BBN approach is neutral.

Being a structured procedure that could be repeated, the BBN process outputs a near exact result whereas the traditional method, being subjective, tends to be inexact and might not be repeatable given the same set of conditions and a different assessor.

Whether or not a risk is acceptable is based on subjective judgment and how the manager feels about the risk level relative to other business objectives. Whereas in the traditional method this decision is entirely subjective, with a BBN it is possible to compare the risk level against a pre planned threshold level, thus taking some of the subjective judgment out of the consideration. In BBN the threshold can be numerically defined.

Once the risk level is determined, the method of mitigation could be fully objective with BBN. This is because the data base would have identified the causal factors and the model would show relationship between causal factors and risk level. Sensitivity analysis would show which causal factors would have the greatest effect on the risk. With this information at hand, mitigation action and priorities could be determined. It is also possible to measure the effectiveness of the corrective action. However the decision on which mitigation action is most attractive to the organization can only be taken by the human, having given due regard to all other conflicting needs.

9.4 Suitability of the model for publication in CAA SMS guidance material

UK CAA have issued a SMS Implementation Plan published on UK CAA website, UK CAA Webpage Safety Management Systems Implementation Plan, which had come in to effect from 1 January 2009, encouraging operators to establish SMS within their organizations within two to three years.

The plan has provided SMS guidance material, Safety Regulation Group: Safety management Systems – Guidance to Organizations[106] as well as SMS Compliance Checklist/ Gap Analysis Form. The Form helps, as name implies, to analyze the differential that exists between the organizations current state of compliance and what was required by ICAO mandate.

It is beneficial to inform the industry on the applicability of the generic model in the context of SMS Guidance Notes. Industry could consider adopting this model as part of its SMS. Publication of information would encourage operators to start experimenting with the concept with a view to eventual adoption within their organizations.

A model specific for an AOC Holder operator would not be suitable for an MRO, although generically they could be similar. Further work would establish if a single model would suit all, or different models would have to be tailored for either individual organizations or groups.

Ideally each operator (or AO) should have a tailor-made model designed to match its operation and local conditions, as they could be different from the generic. For that purpose the organization would have to employ a subject matter expert, ideally on both Bayesian modelling and CAW management. This is because Bayesian modelling is a specialized field and the typical safety engineers coming from a practical background is unlikely to have the aptitude and analytical skills to handle the abstract issues involved. Of course, there may be exceptions amongst them who have the necessary skills and currency, in which case they would be ideal as they already have all the necessary practical experience in safety management.

9.5 Industry willingness to adopt the model

Would the industry adopt this model given it is labour intensive to populate the model? Industry might adopt the model if UK CAA provided the leadership. In the US for instance, FAA has taken leadership in setting up a pilot project involving number of

operators to set up SMS. In UK, CAA might do things differently, but certainly leadership in such important policy changes would help.

Although individually each airline might have independent views and often prefer to reserve their position, when it comes to industry wide issues, they are likely to exercise group behaviour. If the stronger and more vocal operators adopt the model, then the remainder of the industry would fall in line. The cost of introducing and using the model is unlikely to be a deciding factor, even though the industry would be wary of cost escalation of any form in the present economic climate (2010). Timing and reluctance to change are the more likely reasons, even though cost of labour may be quoted as the excuse because in the present economic climate fear of any new cost brings out sensitivities.

Current economic conditions have led to operators shedding labour that does not contribute to revenue generating activities and upholding essential safety related activities. Changes that a new risk assessment method could bring could have long term economic benefits, but it might not be convincing to the operator. In this background any new activity that appears to demand additional labour would be received with disinterest at best or derision at worst. Therefore, they should pause and reflect what the investment and return could be.

During the validation phase of the concept model, the labour cost for researching and categorizing relevant data from the non-relevant, analyzing them and uploading took about three man-months. That is data from a medium sized regional airline, accumulated over a period of 3-years, and one-person (the researcher) working with a set of rudimentary software. With a fully developed model and user-friendly set of software, and safety engineers who are fully familiar with the aircraft system working with data, the labour cost could be less. Eventually, the volume of data to be initially analyzed would determine the overall cost. The effort and labour cost for updating would be very small.

The idea that the new model and its use could be labour intensive is irrational and comes more from the fear of the unknown rather than from reason. The cost of the new system ought to be considered in the light of labour cost to operate the existing safety management and risk assessment methods already in operation in organizations.

There was another fear expressed that a new model may be forced to exist alongside with existing rules and data bases, and that such databases could not be analyzed

easily to match with the taxonomy used in the model. Obviously, the generation gap of a new model and taxonomy and the old database will be a problem. The researcher has encountered this problem, but he has dealt with it as he was willing to take up the challenge as part of the project. On a routine basis, employers might not like to accept that burden and could use it as an excuse to block or delay the advent of new risk assessment methods. The correct way to overcome this problem is through change management. For example the preparation of staffs to handle the new system, the design and publication of data collecting documentation or IT methods that match the new system would help.

If the authority decides to allow operators some degree of self-regulation, then there could be an issue regarding the confidentiality of operator's data when it comes to sharing them with the Regulator. If UK CAA already has access to the operator's information, then this study cannot see what the problem would be in future. However, if UK CAA does not have access, then as part of change management, new rules should be introduced regarding data sharing. If a CEO/AM acts in the interest of safety, as they often declares, then there is no need for them to shy away from the truth.

9.6 Cost benefit to the industry

In the absence of hard data, a qualitative assessment of cost benefits has been made using common sense and informed judgment. This assessment assumes that a fully developed model, together with user-friendly interfaces, is available. It is envisaged that the system would require a modest cost outlay initially (say, around £10,000 for a unit-model) but it would return significant benefits for risk management, in terms of better control over risk status and greater flexibility to conduct engineering operations based on better understanding of the way errors impact on risk level.

- **Outlay.** The organization would have to identify staff complement to operate the system, to uptake existing data and to update the database with new information progressively. One trained person could operate the system, possibly a maximum of 2 to provide 100% cover, but undertaking other safety management tasks It may be possible to utilize existing staff who operate either MEMS or quality management system or if not SMS, as part of extended responsibilities. The volume of extra data to be uploaded and the effort needed appears to be onerous, but in reality, with modern user friendly data exchange interfaces, the data collection processes could be accomplished with relative ease.

- **Archival data.** The analysis and up taking of archival data may be a substantial workload for one or two experts, and the cost would depend on the size of archival data. It was already stated that the researcher spent about 3-months working alone to analyze and uptake 2-years worth of data offered by the participant operator. The elapsed time and effort included time spent in associated tasks such as researching aircraft systems and technical terms related to incident reports on specific aircraft types, as well as trying to comprehend various organizational issues of the operator's maintenance support services, all of which the researcher was unfamiliar with initially. Concurrently, the researcher was also making adjustments to the design of the model in response to his experiences with field data. Therefore, it is reasonable to state here that if the archival data were to be analyzed and uploaded by experts who are already knowledgeable of the aircraft and total environment where these incidents had occurred, then up taking archival data was not going to be such an onerous task to handle, as some opponents of change would like to make out.

- **Transition to self-regulation and reduce cost of oversight inspections.** The model offers organizations an opportunity to exercise a degree of self-regulation. Sincere application of the model in an organization could provide necessary evidence to the Regulator that the organization has the capability as well as the will to regulate itself. If the organization could show through the database and resulting risk assessment that its defence system is effective in containing errors, then it would provide the Regulator sufficient confidence to revise the frequency of oversight inspections in favour of the operator, thus reducing operator's costs. If an operator was accepted as fit for self regulation, then they might be able to save a considerable amount in reduced fees. This does not mean that the legal responsibility for Regulating is passed on to the operator. The Regulator will remain responsible but it should be able to delegate a degree of autonomy to the operator based on evidence.

- **SMS application.** The greater return to the operator will come from using the model as a part of the SMS, in order to determine where risks come from. The way the model has been designed, it provides senior managers a form of "nervous system" to feel the health of their organization's CAW process machinery, and to identify where significant hazards and error generators exist. From his strategic position, a CEO/AM or his deputy would be able to recognize where problems are building up due to human errors that might

upset the dynamic balance of the CAW process. He could then act on that information immediately or allocate appropriate priorities for funding.

- **Minimize cost of accident.** The most important saving that could be gained is in reducing wastage resulting from consequences of an error: the cost of repair or replacement of an engine, recovery from a collapsed undercarriage during a landing, loss of an aircraft, injury or death to passengers and flight crew, or damage to third parties on the ground. This is where the greatest cost savings are. A CEO/AM might say that they have already covered these possibilities by insuring against such eventuality. But even so, with a better knowledge base of risk and ability to reduce it, they would be able to negotiate more favourable premium rates from insurance underwriters.

- **Recognition of good performance**. Recognition of good performance is strategically important for an organization's reputation. This model empowers the organization to make full benefit of good performance, as the model records and utilises good work, i.e. all the flights that the organization has launched with no errors at the end of the CAW process and those sectors completed safely and effectively. This means giving due credit to a well defended CAW process. Existing data collection and risk analysis methods, though aware of this situation, have no means of crediting the organizations for their positive error free actions, and only records negative actions. This is not fair to the operators.

- **Minimize technical admin cost and consultancy fees.** Direct access to evidence as it occurs, will reduce the need for ad-hoc hiring of consultants to investigate what is wrong with organizations and to find solutions. This is in fact the trend nowadays in commercial organizations that minimize in-house specialist technical staffs and rely on external consultancies. The model, as presented here, is designed for the use of technical managers who has a great deal of general knowledge of engineering management but little knowledge of Bayesian Theory. The model will certainly save resources in this respect by keeping all the necessary work in-house and eliminating exorbitantly high consultancy fees.

9.7 Establishing a baseline risk acceptance level

It has been queried if the model could be used to establish a baseline risk acceptance level. Yes, theoretically it is possible, but it is necessary to conduct a wider range of

validation trials to determine the distribution of results across a larger group of operators. Only one validation result is available at present, and that is insufficient to draw any conclusions.

In addition there are two other issues that needed prior resolution. One, the basis on which the risk level is calculated, i.e. is it on the operator's belief or is it on his recorded performance data. The latter draws out the second issue, the size of the population has a significant bearing on the value of the calculated risk level.

If operator's belief was used, then the starting risk level would be the same for all operators, because it is anticipated that they will claim to be operating to a global standard by virtue of the fact that they have adopted EASA regulations and that UK CAA have licensed them to operate as a safe organization.

However, if actual experience was used to compute risk level, then there is bound to be differences between different organizations. A flat distribution would suggest a wide scatter, whereas a peaked distribution such as Normal would indicate a central tendency. If there is a wide scatter, then either each individual organization would have to have its own acceptable risk level as a performance indicator, subject to that it be interpreted together with evidence on its safety performance. A peaked distribution, on the other hand, might suggest that a common acceptable risk level might exist across either throughout industry, or if not across certain groups.

Meanwhile, how would one determine if the level obtained from the model for an individual organization is considered acceptable? To answer this question, first, it is necessary to reflect on the way a surveyor currently determines if an operator's continued airworthiness process activities are safe or not, as explained in Chapter Three, Section 3.13.

If an operator is in compliant with regulation and an oversight audit is satisfactory, then the operator is considered safe. Yet even in such an organization, incidents do occur due to human error. Unless an organization has an uncontrolled history of human error attributed incidents, occasional incident due to human error should not lead to the Regulator declaring that the organization is intrinsically unsafe. Thus, in principle, a human error occurrence is not the main issue in determining minimum safety level; compliance with regulation is the principal criteria. But in a practical scenario, it is compliance with regulation and how human error issues are managed that determines if the organization is performing safely. The risk level obtained from the model becomes a reference level from which variations could be measured.

9.8 Trend deviations

If acceptable risk levels can be established as discussed in the previous section, then it may be possible to establish trend deviations. Naturally it would depend on the distribution profile, and what the variation would mean in practical terms, say, with respect to evidence of safe performance from the organization. At present there is only one result from the validation exercise; this is insufficient data.

Deviations should be allowed, if it is associated with positive management actions to control the risk.

9.9 Key Performance Indicators

Currently statistics on global and national aircraft accidents, MOR, MEMS outputs and trends are used as Key Performance Indicators of the status of health of the industry with respect to airworthiness issues, i.e. how effective safety regulations and management process have been performing. It has been the practice that based on these statistics the Regulator may issue advisory notes to operators on specific areas that need monitoring and control.

Some operators expressed their reservations to the current method of KPI usage as follows:

- The results are always retrospective; suggested improvements are in hindsight, and will be applied retrospectively. Improvements can be seen in future years.

- Rules and regulations based on industry-wide historical data may not be applicable to all the AOs. Information that may be advisory for every operator to ensure no future similar occurrence would be useful, only if the AO use similar equipment or operate in similar circumstances. But in many cases, AOs differ from one another such that generalization may not be acceptable to them.

- Some specific operators have stated that they do not agree with generalized KPI from the national or global authorities' viewpoint. Those AOs do not wish to focus on or monitor one risk influencing factor which may not be relevant to their situation and wishes instead to actively monitor another factor or parameter that is more relevant to them.

The CAW model could help make improvements to the existing system by increasing resolution of influencing factors relevant to certain groups of operators or individual operators.

- Error probability at output could be used as a performance indicator, as well as the influencing factor that mostly impact on the output.

- Through sensitivity analysis available in the CAW Risk Model, it is possible to identify those risk influencing factors that has the most impact on the error probability of output from individual operators.

- Each responsible inspector should come to an agreement with AO, which parameters are important to the AO, and should monitor them.

- The Regulator could then integrate inspectors' reports for their own benefit or to advise any other similar equipment users.

- CAW Risk Model is a dynamic model, and as long as it is used regularly, the user can have almost real time data, as well as the ability to monitor own trends.

9.10 League tables

A question has been raised if individual organizations should be categorized and listed in a league table of achieved risk levels in order to publicize their safety performance. Again, it is too early to comment on this, because there is insufficient information on acceptable risk levels and allowable variations. Once these values are established, then, theoretical divisions, such as gold, silver or bronze, could be established based on quantified values. But the merits of having such divisions should be assessed with respect to actual evidence of safe performance.

It is also necessary to establish if the number conveys a state of safety or the lack of it as observed in practice and what the public reaction to such leagues would be; otherwise the concept of league tables would be ridiculed by those who would be adversely affected by it.

On the philosophy of setting league tables or advocating their publication, this study would prefer to remain neutral; it is a political issue and falls outside the scope of this study. Some operators may be encouraged to develop better safety management as a

result but others might complain that it could affect the commercial side of their business. The concept may be an encouragement to have a better safety culture.

That said, it is common knowledge that there are league tables for the nation's schools and hospitals. Some groups of the public and some experts opposed to this concept, but after several years of their imposition by the central government, authorities and the public in general seemed to have learnt to accept this idea. In this regard, public opinion in general seems to be that the public has the right to know when it comes to the question of risk. Perhaps the same applies to risk to flight safety because flying has become a very common mode of transport for the general public.

9.11 Risk to the CAA of "backing off"

The idea of CAA "backing off" from close supervision of operators arises from a concept that allows an operator to undertake a degree of self-regulation using the CAW risk model as a safety management tool under SMS guidelines. The idea is not meant to absolve UK CAA from its responsibility to the implementation of oversight audits as a regulatory requirement. The phrase "back off" is meant to describe a state where the Regulator relaxes its oversight posture yet retains the responsibility to ensure that operators are complying with the regulation.

If "back off" is exercised with the concept of RBO, then the Regulator exercises a relaxation on the basis of demonstrated low risk. Both parties agree on the standard by sharing base data collected by the subject organization, and the state of continual updating of the risk level. The assigned CAA inspector could have remote access to monitor the organization and he needs to visit the organization only to resolve issues that could not be handled remotely.

There would however be a new task to police that the organization is recording information earnestly and that there is no attempt to manipulate the computation by surreptitious means. Trust and integrity of the operator is paramount here, and it is something that has to be built up. That together with occasional system of checks and balances would give both parties confidence that the system is operating correctly as intended.

The combined effects of the relaxed approach, i.e. remote monitoring, limited checks and balances to ensure that the risk assessment process and self-regulation is functioning as expected, and the reduced oversight program based on risk level,

would be adequate to discount any fears that the "back-off" would introduce new risk to UK CAA.

In an alternative mode of operation, UK CAA might "back off" on the basis of transferring the full responsibility for self-regulation to the operator. Certainly it would require a major change in legislation, and if it did happen, UK CAA is unlikely to be held responsible for operator's lack of compliance. UK CAA might be given a new task of policing the operator's operating the new system properly, and the power to deter any breaches through a regime of penalties. Under these circumstances, the question of risk to CAA would not arise.

A further alternative approach would be the contracting out of oversight audit function to a commercial third party. This approach would be similar to the first approach, except that the cost of oversight inspection might be subject to market testing; thus the operator might get its cost reduced. As to the risk to UK CAA, the risk of backing off is now carried by the third party contractor who has accepted the responsibility for ensuring that the operator is complying. UK CAA carry the responsibility for ensuring that the commercial auditors are properly licensed and are worthy of their role. The third party contractor is accountable to UK CAA. This option too would require amendments to the existing legislation regarding the roles of UK CAA, the operator and the third party auditors with respect to regulatory compliance.

9.12 Relevancy to human factors issues

A discussion on risk assessment due to human error would not be complete if it did not contain some comments on one or two significant human factors issues that are relevant to this study. Improvements to risk assessment techniques would be futile, if insufficient effort was made to comprehend and rectify some of the human issues that either contribute to error generation or inhibit error management. Based on the researcher's critical observations during this study, and information obtained from discussions with subject matter experts, the following comments are made.

9.13 Holistic approach to error management - Health and welfare

Whilst the industry is decisive and effective in mitigating error attributed to shortfalls in design, production, testing of aircraft and related hardware, it is less motivated to resolve causal factors related to the individual. It was seen in Figure 3.5 that issues relating to the physical and mental well being of the people who work in stressful environment are at the centre of basic HFACS framework, yet this is the very area

whose development has been neglected by employers in civil aviation industry. In recent years the emphasis has been in how best to take most out of people to maximize productivity, to increase profit margins and to hire and fire people at will in order to manipulate labor to meet commercial objectives.

The message conveyed in this section is that it is the human in the loop that makes errors in design, production, testing, and maintenance, and planning how these activities should be done. Part of that is the limitation of knowledge, leading to failure to account for certain conditions that the equipment would be subjected to during service. Another part is his state of mind when working with existing knowledge that prevents him from using his knowledge.

CHIRP/MEMS database[107] reveals that a large proportion of recorded human error incidents were people related, as opposed to process related. Closer examination of data reveals that some errors are related to individual performance that demands on mental faculties of memory and assimilation of information under pressure. For example, having analyzed 270 cases of installation error of which 205 were reported under MEMS and 65 under MOR, CHIRP/MEMS[117] attribute 39% of installation errors reported under MEMS to individual performance, and 49% of the installation reported to UK CAA under MOR in year 2007. Memory lapse accounts for 6% of individual performance lapses, whilst personal fatigue accounts for 12% of performance lapses.

Subject experts have often pointed out that despite publicity and local initiatives to disseminate information this pattern was repeating year on year. Part of the reason may lay in the authorities failure to recognize it as a significant problem and give due attention to investigate and alleviate the human factor issues that lead to the deterioration of mental faculties.

9.13.1 Role of serotonin deficiency

The role of the neurotransmitter serotonin in memory functions, assimilation of information and normal mental faculties is well understood by the medical profession[110], though the general public has little comprehension of it except the general idea that the chemical puts the people in a good mood. During the course of this research program, the researcher had the rare opportunity of closely studying a case of loss of memory and difficulty to assimilate information of a person who was employed outside an aircraft environment. The case was traced back to the inception of the problem, and followed its real time diagnosis and cure. With the permission of the patient the case is cited here, under the principle advanced by Yin (2009)[92] (see

Section 6.5) regarding the use of single case histories in soft science research. Through following up this case history in real time, the researcher's curiosity was aroused that led him into researching relevant scientific research papers in the medical field, and to discuss relevant issues with medical professionals . This section of the report is written from the knowledge so acquired, for the benefit of those in aeronautical profession researching into causation of human error, in order to open up their horizon beyond the world of aircraft.

Whilst serotonin makes people feel good according to the popular belief, deficiency in serotonin, by way of imbalance from what the nature intended, could cause significant deterioration of memory functions and mental faculties. The imbalance, usually a reduction in the level to below the norm is clinically referred to as a depression, meaning a depression of serotonin level in the brain, and NOT a case of losing one's happiness according to the popular misconception. Obviously, depression of serotonin could create an unhappy mood, which is a symptom, which then results with further depression of serotonin level, causing a vicious cycle from which a person might find it difficult to come out unless the cycle is broken by intervention. Intervention to restore balance is possible, but it will take some finite time, and with timely treatment the person will get back to normality.

Serotonin in the brain acts like e-mail to send information from one brain cell to the other. When serotonin is deficient, it creates a condition that is similar to not having a 2-way medium of communication; once the 2-way flow of information between brain cells is impeded or blocked, it inhibits memory functions, which easily leads to not coping with information flow, to confusion and to irrational thinking. More of this could be read in relevant medical literature available in public domain.

From a human error perspective, this phenomenon has much significance. When engaged in technical work that requires concentration and assimilation of information rapidly, analyzing and acting on them, sufferers of serotonin deficiency could be most susceptible to making errors as they begin to lose memory functions and analytical reasoning skills required for the diagnosis of engineering and management issues related to their task. The deterioration would get exacerbated if they were put under time pressure, e.g. the knowledge of approaching or imminent departure schedule if they are working on a pre-flight task. Under serotonin deficiency, even a simple task of searching for some information on the computer or in an AMM could be perceived by the sufferer as a major task that he would not be able to handle, as he loses his situational awareness, orientation, energy and the will to make the body act. And strangely, according to the consulted medical professionals' opinion, the loss of will,

forgetfulness or tendency to distraction from the task has been attributed to the brain's own natural defence mechanism from overloading it.

Ironically such people may outwardly show no physical symptoms, and more so in a social setting where they might be observed and therefore show the best behavior. This phenomenon may explain why sometimes, the most trusted and experienced engineers and line managers, some of whom have had very long service in the profession, make otherwise inexplicable errors. In any social group and community there might be a proportion, i.e. a norm for the general population, which might be at varying levels of stress close to their individual stress thresholds, with different people in the group affected at different times. It might explain the reasons why, despite all other palliatives, the same types of person-related error get repeated, and why the rate of human error arising continues unabated, year on year[105, 107]. It was interesting to reflect on an open question that Head of Chief Surveyor's Office, UK CAA, posed to the researcher at the beginning of this research study, and left unanswered at the time, "How could a fully qualified and experienced LAE leaves out a shim when fitting a wheel on to an aircraft?" Would a simple statement like, "He forgot, despite his experience" fits the answer? If he did, he might not have been at fault willingly, because he might have been internally suffering from stress. This explanation may sound incredible, but in fact, it is perfectly possible for a sufferer of serotonin deficiency.

9.13.2 Role of stress and loss of sense of welfare

According to Royal College of Psychiatrists[111] a key contributor to depression is excessive stress from their life style, social and domestic pressure, exacerbated by work place stress, and the way they interact with a persons' sense of fear, security, worth and well being. Since the susceptibility to depression is a function of many variable parameters such as a person's inner make up, body chemistry, age, and stress threshold, it is extremely difficult to predict when a person might be going through an early stage of depression. Experience of the person or their trustworthiness does not come into the equation, when the person is suffering from depression. If anything, his awareness of his status in the organization and his realization that he is not coping well could make matters worse for him, despite the image that he would like to project.

Standard guidelines from safety management literature, such as ICAO SMM, Doc 9859[38], recommend that engineers observe if work colleagues change their normal habits, change mood, beginning to make simple mistakes at work or show signs of

forgetfulness. These may be the tell-tale marks, but in a CAW process, that is critical to the safety of the aircraft and its passengers, reliance on a colleague to watch the behavior of another is somewhat a simplistic, though tactful, approach to a serious problem. In fact it is unlikely that a colleague will report on another workmate whom he likes and only consider reporting someone who is disliked according to group behavior, sometimes times for wrong reasons. The case study A 07/026_1 (Error 2) discussed in Appendix 6 is one such case.

Furthermore, a Director of another airline cited a case of a senior aircraft worker who was about to be dismissed for a human error related violation when it was learnt at the eleventh hour that he had been suffering from serious health and welfare issues for long time, unknowing to the management. The Director regretted not having had adequate insight to people's welfare issues, but in mitigation expressed the view that under current legislation and trade union relationships, there was little the organization could do to cross the boundaries between a person's privacy and organizational welfare and task needs.

9.13.3 Development of interventions through new research

Whilst much attention and effort is made to monitor the health and welfare of flight crew, ground staff who manage and implement CAW processes receive much less attention and authorities' recognition in this respect, by way of welfare services for the staff at work place and improving working conditions and security of employment. In fact the current tendency of organizations is to shed any support services that had been previously established to deal with health and welfare issues of personnel. The usual reason given is that privacy, human rights and labor laws, more likely the trade union influences, prevent authorities from acting on health and welfare issues of individuals. In fact the lack of relevant statistics of evidence is quoted by senior managers for not doing anything positive in this regard.

Fear of job security alone is a strong reason for people not to come forward to seek assistance. The intangibility of information that a sufferer might present as evidence could be open to disbelief or criticism is a major inhibition. Therefore this study observes that there should be a better industry-wide understanding of the exact mechanics of the human body undergoing stress, the serotonin deficiency factor, and resulting susceptibility to make human error. The overall interactive phenomenon should be treated as a latent natural hazard common to all people and not to the failing of one individual human who was forced to cross his stress tolerant threshold by the circumstances.

As part of this research study the National Authority's attention has been drawn to the general issue of health and welfare, pointing out that "forgetfulness" is a significant causal factor, and perhaps there may be some deficiencies in the way the aircraft workers' health and fitness is assessed. The response has been that the Authority and approved organizations are currently working to the regulation and that there is no evidence to raise an alarm. However the point being made in this thesis is that evidence may be there in the data already accumulated industry wide, and in the databanks of appropriate professions engaged in research into this phenomenon. If they have been largely ignored because industry was trying to protect itself from expenditure perceived as nugatory, then this is an opportune time to review that previous establishment posture. No amount of sophisticated risk assessment will help to reduce human error if nothing worthwhile is done at the fundamental root level, where conditions for committing errors begin. In this context CAW Risk Model would help to record and discriminate between the importance of causal factors, but it will not stop or reduce risk unless the authorities concerned are properly educated and are willing to act on acquired intelligence.

It is quite understandable that an authority trying to work for a limited budget does not wish to start unaffordable research in the short term, but in the long term it would be a positive and constructive action to start, even some low profile research studies to see how best to reduce errors arising from this causal factor. Approved organizations too ought to revive a "sincere interest in people" instead of interest in people as PR stunts for recruitment drives.

Recognizing the relationship between human-fatigue due to extended work hours and risk to flight safety, International Federation of Airworthiness (IFA) has circulated a paper[112] on its website that proposes the need for the industry recognition of hazards of extended work hours. The paper proposes the formulation and establishment of a set of standard guidelines and procedures that may be implemented industry wide, at least voluntarily, in order to mitigate the risk contribution from this cause. Following the same theme, IFA had presented further papers on human fatigue at the IASS 2008[118] and at Aviation Fatigue Management Symposium educating aviation industry collectively on the hazards of human fatigue and the need for Fatigue Risk Management System.

From Health and Safety Act viewpoint too, IFA proposal makes good sense; it resonates with the same spirit of The Examiner, Irish News, which reported an

accident to a mechanic working on a Ryan Air aircraft, who lost his arm at a moment of distraction after allegedly working on the aircraft for 14-hours[113].

This research study too reiterates that current regulation may be inadequate on the question of health, welfare and fitness of aircraft engineers from a human error reduction point of view. Therefore, perhaps, the National Authority should take a more holistic view of the entire topic relating to those who are engaged in CAW process activities; they should initiate suitable further research to gather evidence to justify investment in people in order to mitigate risk from this universal hazard common to people.

9.14 Parallel advances in the social order

It has come to light during research interviews that the reluctance of some operators to cooperate with the study is attributed to a sense of fear and insecurity. It was the fear that by having an error data base, they would be under legal obligation to provide information to those who have the legal right to know, whereas if they did not keep a database they would be free of such threat. They saw the presence of the model together with its database as a threat to their security and commercial interests.

Two specific groups with the right to access data are insurance underwriters who provide insurance cover and the other, the legal profession who represent victims of aircraft accidents and incidents. There are others interested in data; civil police investigating any criminal activities, individual employees or their trade unions that represent them on industrial disputes, such as job evaluations issues or unlawful dismissal by the employees, and the Inspectorate for Health and Safety at Work.

The trend in new legislation that compel organizations to be more vigilant on safety issues and to release pertinent information to the law courts or anyone else who has the right to know is bound to stay with us. Latest legislation on Health and Safety relating to corporate manslaughter and top executives individual responsibility to exercise “Duty of Care” for those who come under his sphere of responsibility is a case in point. Such changes in law and current trend to make organizations more accountable to the public are a part of the natural progression of social order that we live in.

This fear underpins one of the strong inhibitions to the open reporting of error, and authorities’ reluctance to share error data with external bodies as they fear that they could be open to legal liability claims or undermine their commercial interests.

Meanwhile other operators who saw open reporting as constructive and progressive reacted differently. Apart from the positive contribution, they supported its role in promoting flight safety as well as providing critical information to the management enabling them to prioritize investment and to timely resolution of issues that undermine safety.

Therefore, no matter how well and sophisticated the business of error management and risk assessment is developed, it can only work on the basis of obtaining correct data. And if the data is not forthcoming due to the current social order with respect to legal liability for error, then the society must ensure that the frontiers of the social order too are advanced in harmony with the demand for better methods to assess risk. Related sectors in which such advances to be made are in resourcing and taxation, tort and contract laws, health and safety, industrial relations, business management, to identify a few. This study is of the opinion that it is up to the HM Treasury to influence the respective government departments to make such progress, just as the way it would like UK CAA to make improvements to the way risk is assessed in civil aviation.

Chapter Ten

Conclusion

10.1 Introduction

A computer model based on Bayesian Belief Network concept has been designed and developed to assess risk due to human error in organizations undertaking continuing airworthiness processes. The model works together with a database of human error occurrence and their causal factors. The model is applicable to both passenger and cargo aircraft CAW process operations. The model is generic and may have to be modified to suit specific organizations.

In order to convert the model to a practical tool, it would require further development such as the provision of user-friendly interfaces, packaging into a commercially attractive product, e.g. a "software package" for use with a desktop PC or a laptop computer, and the provision of a product support system.

Concluding the research study, this Chapter will now review its achievements relative to research objectives, highlighting strengths and limitations of the model in industrial application. The chapter is rounded off with a statement of the study's contribution to knowledge and recommendations.

10.2 Model's output and use

- The model outputs prior probabilities of error at critical nodes, their consequences and costs. The output represents the error and non-error performance of an approved organization. Given that errors occur, if they are under control and managed, then the risk level remains tolerable. The prior probability represents the risk level of the organization in a dynamically balanced steady state.

- By continual updating, the model provides new risk levels that may be either within tolerable limits or without. The Regulator, in consultation with the organization, should determine the acceptable steady state level and tolerable variation.

- Similarly, by monitoring the results and causes, it is possible to establish trends that can be used to control adverse trends.

- In prediction mode, the model could be used to determine the effect of undetected error at any point in the core CAW process or peripheral subsystems on the end product.

- The use of the Risk value as a single number has been replaced by a matrix of Probability of Error vs Probability of Consequences or Probability of Cost Level. This takes into account the fact that an error probability at the point of aircraft dispatch could have different possible outcomes.

- The range of information provided by this risk model would be of benefit to a CEO/AM than the availability of a single risk number. Given the full range of matrix output, trend data, prediction facility and hot-spot monitoring of outcome to error occurrence, they can select and focus on the performance indicator that is most relevant to their organization.

10.3 Validation trial

- Validation trials confirmed that it was possible to use the model in conjunction with historic field data files from a participating aircraft operator. However Flight Consequences predicted by the model, based on data for 34,000 sectors, proved to be were more pessimistic than the operator's expectation.

- Alternative data based on operator beliefs, that it was operating to global safety levels by virtue of following globally accepted safety standards, returned outputs consistent with known global safety levels. It confirmed that the model was functioning correctly. However the belief would hold true only if the operator had flown around 3M sectors and experienced pro-rata number of incidents or fewer.

- The 34,000 sectors and the error incidents experienced could not be regarded as achieving global safety level, even though it was perfectly valid to acknowledge that the operator was operating to global safety standards.

- The trial confirmed that operating to a global safety standard such as EASA regulation does not necessarily mean actually achieving the global safety rate.

Despite operating to regulation, errors could occur that might contribute to a higher probability of accident.

- The result confirmed the differential between the belief and the reality of higher risk, a situation that is already generally known in the industry. Licensed aircraft engineers acknowledge that demonstration of compliance with regulation alone does not provide full safety, because despite regulation operators occasionally fail in their safety performance. This is the basis for continual audits.

- Provided the achieved risk level is acceptable to the Regulator and any adverse trends are properly managed and controlled, there is no reason why the operation could not be continued. This is the common sense approach, which supports the case for safety management system.

- On the question of inputting either belief or actual data:

    - If safety is paramount, the risk level based on actual experience should be adopted. That is the safe approach that would give confidence to the operator, to the Regulator and the public, and moreover harmonizes with the ICAO guidelines that have been adopted by industry to this date.

    - The risk level based on belief may have to be used if actual data is not available, e.g. in a new organization without a previous history.

    - Beliefs based on claimed achievement of global safety levels should be tested against organization's historical experience and size of database.

- A common sense approach is that risk level based on experience should be used, not as an absolute value, but as a reference from which improvements could be measured or deterioration could be monitored and corrected. It is an indication of the reliability of the human in the CAW process, and not necessarily how reliable the eventual flight is. This is because there are factors other than CAW, which contribute to safety but not taken into account in this analysis, e.g. flight crew action that would defend the consequence of a human error in CAW.

- Acceptance or rejection of the human error contribution in CAW, e.g. in terms of probability of errors and consequences, depends upon the threshold values

that could be set initially by the organization itself in consultation with the Regulator.

- To implement this process industry-wide, there should be an industry standard bench marking to establish threshold levels and allowable variations. Further development work may be required to establish these criteria.

- The output from the model is sensitive to the size of the population. Larger the population, the more reliable and smaller the estimated risk levels become. This means, those organizations that do not have a large historical database are likely to be judged as less reliable, requiring more frequent or more thorough oversights, compared with others that have a long history of good safety performance.

10.4 Air transport application

Regarding the applicability of the model in air transport industry in relation to either RBO concept or ICAO mandate on SMS:

- The model provides a management tool that could be used in the implementation of risk assessment tasks within a safety management system and implementation of RBO concept at strategic level.

- If the Regulator wishes to adopt the model for RBO implementation, then it would be prudent that the final form of the CAW model is agreed with the operators. In this case, Regulator would have to take leadership, conduct a pilot study in participation with a representative set of operators, for establishing either benchmarks or threshold values of risk, and allowable variations.

- A pilot study would also provide the opportunity to validate the model in industry as a tool for exercising some degree of self-regulation and its use in SMS.

- Relief from current oversight regime might be possible if operators are allowed to exercise a degree of self regulation as part of their SMS, using risk assessment models based on BBN concept. In such a system, the Regulator would have to exercise an audit function to ensure that the operator is faithfully adhering to the principles of recording all errors and accountability for them. The Regulator should be legally empowered to penalize offenders.

- Once industry consensus on the use of the model was obtained, information on the model could be included in SMS guidance notes, so that if any operator is willing to adopt it, then they could do so voluntarily within the current framework of SMS implementation.

- Implementation of RBO concept is within the Regulators prerogative whereas the use of the model in SMS is left to the operators and associated approved organizations. The model does not dictate policy decisions on acceptable risk levels and variations, but helps to guide managers in formulating a policy.

- If the model is to be utilized in industry, then it would require further development, in the areas of database construction and management, user-friendly interfaces, and display of outputs. Such developments are essential in order to reduce the labor costs in the application of the model.

10.5 Differentials in roles and scope

- The CAW Risk Model is suitable for use in both passenger and cargo air transportation environments.

- The air cargo subset of parameters caters for cargo handling data. A similar subset could be added to account for passenger handling, vide evidence in UK CAA Paper 2009/05[105] that errors in passenger role equipment and emergency cabin equipment leads to airworthiness issues.

- Provision has been made for the model's use with either fixed wing or rotary wing aircraft.

- Subsystems, nodes and other parameters could be added or truncated as necessary depending on application or change of operating conditions.

10.6 Strengths

The study confirmed that the model meets the desirable criteria for a risk assessment model as identified in PH report.

- **Data driven.** The model is primarily data driven, but it is also possible to use beliefs based on individual opinion. Hence it is more robust, transparent, open

to scrutiny and unambiguous than traditional methods based on subjective judgment alone.

- **Mathematical basis.** Risk is based on conditional probabilities calculated using Bayes' Theorem, which is a mathematical formula.

- **Quantitative Output.** The output is quantified.

- **Better assimilation of information and more accurate computation.** The model estimates probabilities for a wide range of operational conditions much better than a human could ever do.

- **Cost Data.** The model provides an indication of what errors cost the organization. This cost utility may be very useful to the corporate business managers.

- **Utility for AM/CEO.** The model is a management tool for AM/CEO and high level managers. Once the statistical case is known managers could take their own decision, according to their personal judgment and experience, using model output as a point of reference. The output is a guide to AM/CEO and not a dictate.

- **Improved resolution.** The resolution of the network could be adjusted, and the resolution could be increased or decreased by modifying the network.

- **Existing Data.** The model uses existing data as far as possible. Absence of data is not critical to calculations, but if data is available then it makes the calculation more accurate.

- **Widening database.** If a comprehensive dataset is not usually collected and recorded, then the model's provision for them encourages the organizations to maintain a better set of data in future, thereby improving fidelity of results.

- **Mature organizations.** Mature organizations that have an established operating history and existing database could start off with hard evidence data.

- **New organizations.** New or small organizations with no existing database could start off on the basis of best estimate and expert assessment, until these are gradually replaced by hard evidence data.

- **Types of Error.** All observed CAW Errors regardless of their importance can be recorded. Thus innocuous or incipient errors at the "bottom of the error iceberg" are also taken into account, even though under normal circumstances they are ignored as insignificant.

- **No Error Flights.** Recording of No Error flights or flight preparation gives credit to the organization for safe performance. It would provide a true probability of error, whereas errors-only recording would give a biased, pessimistic view of the organization.

- **Causal Chain or Random Fragmentary Data.** Causal chain data resulting from full investigations provide best evidence. Where a full causal chain is not available or investigation not fully followed up, fragmentary information can be utilized. The model was found to work with fragmentary data, and the assumption is that they are random events that occur in isolation.

- **Effectiveness of Defences.** Effectiveness of defences can be determined with this model because it allows defences to be recorded. It is possible to increase the resolution of the relevant nodes to determine which defences are more effective than the others are.

- **Consequences.** Provision has been made to record a wide range of consequences of an error observation.

- **Crossing management barriers.** As the model is based on causal chains, the model encourages full causal chain investigation providing an opportunity to cross management barriers.

- **Policy transition**. The model provides the link between different layers of organization, helping to identify points where safety needs conflict with commercial needs.

- **Provides sensory system.** The model provides the senior managers with a sensory system, to detect critical trouble spots, and to take timely actions to correct them.

- **Opportunity for self regulation**. If utilized in their organizations, the model provides the operators an opportunity to undertake self-regulation, and to win over the trust and confidence of the Regulator. Thus, an operator could benefit by minimizing Regulator's involvement in extensive oversights. Operators are encouraged to be self critical on areas where compliance has been less than adequate.

- **Better management of oversight resources.** The model provides the Regulator an opportunity to better manage their oversight inspection resources, i.e. to match resources to the level of risk of individual organizations.

- **Unknown conditions.** The model cannot assimilate unknown conditions, only those pre-programmed into the model. For the assessment of risk due to unforeseen events, some intuition is needed and it can only be done with human skills and a degree of subjectivity.

10.7 Limitations

- **Poor cooperation from managers.** A key strength of the model is also seen as a potential weakness. The causal chain type investigation might make managers feel exposed since most errors have a root cause in the organizational level influencing factor. Therefore self protection could come into play, and they might reject a concept that makes them vulnerable.

- **Management discretion on extent of investigation.** The categorization of errors, decision to investigate or not investigate, to report or not to report are functions still controlled by human operators and managers.

- **Not conducive to tactical level assessment.** The system provides a means for handling strategic level risk assessment, but it is less applicable to tactical level assessment, unless the model is already pre-programmed.

10.8 Achievement of research objectives

- The primary objective has been achieved satisfactorily, which was to design a generic Bayesian model that could assess risk due to human error in the approved organizations that undertake CAW processes of air transport.

- The model could be used as a risk assessment tool in SMS in so far as strategic risk assessment and monitoring is concerned.

- It can be used for tactical risk assessments about the organization and process, by way of predictions, provided prior conditions have been integrated into the model.

- The CAW Risk Model does not support tactical risk assessment decisions relating to specific aircraft systems. It was not the intention. For that, expert judgment based on experience and evidence from system diagnostic tools and processes should be used.

- The model can be used in supporting RBO concept, in so far as the issue of determining urgency and resource allocation is concerned.

- The secondary objective of finding an alternative means of satisfying meeting Regulatory requirement is part-satisfied. The following qualifications are made to highlight other related issues that could not be addressed within the scope of this research study.

    - Utilizing the model, an organization can embark on a program of continual self-regulation even to a greater depth than possible with existing method of oversight audits.

    - The model's effectiveness will depend on the honesty and integrity of the organization.

    - Where openness is missing, and the operator acts purely on its commercial instincts the concept could fall into disrepute.

    - If self-regulation were to be sanctioned, then the process would have to be audited by the Regulator, and they should be legally empowered to enforce penalties against breaches.

    - Any changes of Regulatory compliance audits would have to be preceded by change of legislation.

10.9 Contribution to knowledge

- Application of the BBN concept to assessing risk in civil aviation safety management in a wider scale has not been hitherto attempted. This could be due to lack of vision as how best to represent the wide range of influencing factors, and their complex interactions, in one network. Overcoming this blockage, the CAW Risk Model has paved a way by offering a heuristic approach that has been tested and subjected to limited validation.

- This research study led to the recognition that the statistical solution to the analogy of Swiss cheese in Reason Model lay in Bayes' Theorem on conditional probability. This relationship has not been specifically mentioned in any relevant literature although the analogy has been made qualitatively. To that extent, this is new knowledge.

- It is possible to quantify risk due to human error as a statistical probability. In fact the achieved risk values may be more severe than what operators believe may be happening in their own organizations, as they have been distracted by collective global flat rates and design reliability levels to the detriment of their own standards.

- There is no simple, single solution to the problem of assessing risk in civil aviation. The methodology depends on the circumstances and purpose. This research study addressed a method that is more appropriate for strategic level risk management. Though the model is designed for CAW environment, its concept could be applied to other specialist areas of civil aviation such as flight operations or any other Regulatory regime.

- As a by-product of this research study, this thesis presents a simple, systematic, step by step guide to the design and use of a BBN, which has not been available to new comers to this subject, particularly to those such as research students who wish to develop their knowledge by self-effort.

- This study has also introduced a rule of thumb method to check if a complex BBN using proprietary software (whose algorithm is not in public domain) is seen to be calculating prior conditional probabilities correctly, a technique that has not been encountered in literature.

10.10 Recommendations

10.10.1 Publication of CAW risk model information in SMS Guidance Notes

Under Section 10.4 it was concluded that the risk model could be used by air operators as part of their SMS. In doing so, they could use the model as a supporting tool to exercise a degree of self-regulation and to measure its efficiency. Under its current policy of encouraging operators to implement ICAO mandate for SMS, UK CAA has published guidance note on SMS. This study recommends that information about CAW Risk Model should also be published in the same SMS Guidance Notes as an example of a risk assessment and quantification tool. Operators would then be free to adopt the model if they wish to do so.

10.10.2 Extended validation trials with a larger group of operators

Industrial application of the model may require UK CAA approval as well as consensus from civil aviation industry. Although the model has been tested and validated using one aircraft operator's field data, it would be prudent to extend this validation exercise across a larger group of operators to gauge their reaction as well as to gain their confidence in the use of a new risk assessment method. Such trials should be used for the benchmarking of threshold levels and establishment of allowable variations (Sections 9.7 and 9.8). It is recommended that UK CAA should consider taking leadership for conducting extended validation trials amongst a larger group of operators.

10.10.3 Research into human fatigue that leads to human error

Section 9.13 discussed the significance of human in the loop of the CAW process and the need for physical health and mental welfare in order to minimize human error. Whilst organizations are ready and willing to invest on inanimate HF issues such as aircraft design or procedures by way of mitigation, they are less enthusiastic to invest on improving the physical health and mental welfare of its staff, especially those at the workface. Lack of evidence and data is often quoted by those responsible, but this study noted that evidence is in fact available, but it is not systematically documented or analyzed.

Part of the shortcoming in the current state of play is that neither authority nor approved organizations takes responsibility to lead research into this area or to come up with proposals to improve the worker's welfare and working conditions. In its

absence, IFA have taken an initiative in the form of publishing and promoting research papers on Human Fatigue at Workplace, at learned bodies or conferences, but no organization that has executive powers have taken steps to take forward IFA's recommendation. Consequently, this study recommends that UK CAA should take the lead on research into the relationship between human error at work and the health and sense of well being of those who work in the CAW environment. The purpose of such research should be to determine the required level of investment on people in order to reduce human error and promote flight safety

References

1. Reason, J. and Hobbs, A. (2003). *Managing Maintenance Error: A Practical Guide*, reprint 2004. Ashgate Publishing, Aldershot.
2. NTSB (2001). Loss of Control and Impact with Pacific Ocean Alaska Airlines, Flight 261 McDonnell Douglas MD-83, N963AS, about 2.7 miles North of Anacapa Island, California January 31, 2000. *US National Transportation Safety Board Abstract AAE-02/01.*
3. NTSB (1989). Aircraft Accident Report – Aloha Airlines Flight 243, Boeing 737-200, N73711, near Maui, Hawaii, 28 April 1988. US National Transportation Safety Board.
4. UK AAIB (2007). *Report on the serious incident to Boeing 777-236 G-YMME on departure from London Heathrow Airport on 10 June 2004*. *Report No: 2/2007.* Air Accidents Investigation Branch*,* Department for Transport, United Kingdom.
5. PlaneCrashInfo.com database. At http://www.planecrashinfo.com/cause.htm (accessed 25 July 2010).
6. UK CAA (2008). *CAP 780 Aviation Safety Review*. UK Civil Aviation Authority, Gatwick.
7. Eshati, S. (2006). *Critical analysis of maintenance error decision aid (MEDA) and human factors analysis and classification system (HFACS-ME) in aircraft maintenance,* MSc Thesis. Cranfield University, September 2006.
8. Braithwaite, G.R. (1998). *Australian Aviation Safety - A systemic investigation and case study approach*, Doctoral Thesis, Loughborough University, April 1998.
9. BEA (2002). *The BEA Report on Accident to the Air France Concorde F-BTSC on 25 July 2000 at La Patte d'Oie in Gonesse (95)*, January 2002. Bureau de Enquetes et D'Analyses pour la Securite de L'Aviation Civile, Paris, France.
10. UK AAIB (2010). *Report on the accident to Boeing 777-236ER, G-YMMM, at London Heathrow Airport on 17 January 2008. Report No: 1/2010.* Air Accidents Investigation Branch*,* Department for Transport, United Kingdom.
11. Hobbs, A. (2008). *An Overview of Human Factors in Aviation Maintenance, Report: AR-2008-055*, December 2008. Aviation Research and Analysis. Australian Transport Safety Bureau.
12. UK CAA (2010). *CAP 393. Air Navigation: The Order and the Regulations.* 3rd Ed. 14 April 2010. UK Civil Aviation Authority, Safety Regulation Group, Gatwick.

13. Hampton, P. (2005). *Reducing administrative burdens: effective inspection and enforcement,* March 2005. HM Treasury, HMSO 2005.

14. ICAO. *Annex 6 to the Convention on International Civil Aviation, Operation of Aircraft. ICAO Article 44 Convention, Document 7300.* International Civil Aviation Organization.

15. Leach, H. (2005). Maintenance Error Prediction Modeling, *Proceedings of the 36th Annual International Seminar of International Society of Air Safety Investigators.* Texas, US. Sep 2005. ISASI, Sterling, VA 20164.

16. Simmons, A. (2002). *Maintenance Error – An Overview and Proposal for Error Management in Numerical Airworthiness Terms*, MSc Thesis, University of Bristol (2002).

17. Marsh, D. (2007). *CAA Regulatory Oversight Weighting Index (ROWI)* – An unpublished internal paper, Southern Region Office, UK Civil Aviation Authority, Gatwick, 2007.

18. Luxhoj, J. T. (2003). *Probabilistic Causal Analysis for System Safety Risk Assessments in Commercial Air Transport.* Dept of Industrial and Systems Engineering, Rutgers University, USA, 2003.

19. IATA (2008). *Leading Change – IATA and Its Priorities.* International Air Transport Association, at http://www.iata.org/about/ (accessed 12 March 2008).

20. IATA (2007). *Annual Safety Report 2006*, issued April 2007. 2006 Ed, International Air Transport Association, Montreal.

21. IATA (2008). Improving Air Cargo Competitiveness. Internet website data at http://www.skycontrol.net/organisations/iata-improve-air-cargo-competitiveness (accessed 31 March 2008).

22. Bender, M and Wells, D.J. Fleet supportability and aging aircraft. Air Line Pilots Association, International, Herndon, VA 20172

23. Roelen, A.L.C., Pikaar, A.J., Ovaa, W. (2000). *An analysis of the safety performance of air cargo operators*. Report NLR-TP-2000-210. March 2000. Civil Aviation Authority of the Netherlands.

24. NASB (1994). *Aircraft Accident Report 92-11, El Al Flight 1862. Boeing 747-258F 4X-AXG Bijlmermeer, Amsterdam, October 4 1992.* Nederland Aviation Safety Board, Raad Voor de Luchtvaart (Council for Aviation).

25. Reyd, P. (1999). Dutch government rocked by parliamentary report into 1992 El Al air crash. 27 April 1999. World Socialist Web Site at http:www.wsws.org/articles/1999/apr1999/hol-a27.shtml (accessed on 7 July 2010).

26. Scott, M. (2009). Despite 2009 Accidents, Flight Safety is Improving. Spiegel On Line International, 27 July 2009.

27. Jensen, D. (2003). How an Irish Career seeks More green. *Avionics Magazine*, 1July 2003.

28. ICAO. *Document DOC 7300 Introduction to 9th Edition, Corrigendum 26 November 2007.* Convention on International Civil Aviation.

29. ICAO. *Document 9713. International Civil Aviation Vocabulary – Volumes 1-2*, 2nd Editions 2007. Convention on International Civil Aviation.

30. EASA. *European Commission Regulation (EC) No 2042/2003 of 20 November 2003 Article 2.* European Air Safety Agency.

31. Heinrich, H.W., Petersen, D., Roos, N. (1980). *Industrial Accident Prevention: a Safety Management Approach.* 5th Ed. McGraw-Hill, New York (First edition 1931).

32. Allen, J., Rankin, W., Sargent, R. Human factors process for reducing maintenance errors. AERO Magazine-03, Boeing Commercial Airplane Group, Seattle, at www.boeing.com/commercial/aeromagazine/aero_03

33. HM Treasury (2005). Meeting the productivity challenge 14. *Budget 2005*. Chapter 3, Para 3.32.

34. Pidgeon, N. F., Hood, C., Jones, D., Turner, B., and Gibson, R. (1992): Risk Perception in Risk Analysis, Perception and Management: Report of a Royal Society Study Group, 1992 The Royal Society, pp 89-134.

35. Cabinet Office (2002). *Risk: Improving Government's Capability to Handle Risk and Uncertainty. Annexes.* Cabinet Office Strategy Unit Report, November 2002.

36. Douglas, M. (1992). *Risk and Blame: Essays in Cultural Theory*. Routledge, 1992

37. House of Lords Sub-Committee on Science and Technology, Third Report, 1999.

38. ICAO. *Document DOC 9859. AN/460 Safety Management Manual,* 1st Ed. 2006. International Civil Aviation Organization. Chap 5.

39. HSE (2010). Glossary of terms. *HSE Handbook Reducing Risk – Protecting People.* Health and Safety Executive, Bootle, Lancs, UK.

40. CIAIAC (2008). *Accident Involving aircraft McDonald Douglas DC-9-82 (MD-82) Registration EC-HFP, operated by Spanair, at Madrid – Barajas airport on 20 August 2008. Interim Report of A-032/2008*. Commission for the Investigation of Civil Aviation Incidents (CIAIAC) of Spain.

41. ICAO. *Document DOC 9734 AN/959 Safety Oversight Manual: Part A – The Establishment and Management of a State's Safety Oversight System.* International Civil Aviation Organization.

42. FAA. *Code of Federal Regulations: Part 25 Airworthiness Standards: Transport Category: Airplanes.* Federal Aviation Administration, Dulles, VA 20166. At http://www.faa.gov/search/?q=Part+25+airworthiness+standards (accessed 2010).

43. EASA. *CS-25. EASA Certification Specifications for Large Aeroplanes.*

44. Bristow, J.W., Irving, P.E. Safety factors in civil aircraft design requirements. *Engineering Failure Analysis,* Volume 14, Issue 3, April 2007, Pages 459-470.

45. ICAO. Document 9734 AN/959: Safety Oversight Manual.

46. FSF (2010). Tupolev-154M 10 April 2010. *Flight Safety Foundation, Aviation Safety Network*, at http://aviation-safety.net/database/record.php?id=20100410-0 (Accessed August 2010).

47. CHIRP (2010). *Feedback, Bulletins of CHIRP, at* http://www.chirp.co.uk/feedback-list.asp?fb=AT (accessed 2010).

48. UK CAA (2006). *CAP 642: Airside Safety Management.* Safety Regulation Group, UK Civil Aviation Authority. Gatwick.

49. *Aviation Disaster: Investigating the Causes, Resolving the Claims.* Proceedings of conference by AVICON, rti, IMC, Cozen O'Connor, INCE & Co. on 9 October 2008.

50. UK CAA (2009). *CAP 382: Airworthiness Authority under the Mandatory Occurrence Reporting System.* UK Civil Aviation Authority. Gatwick.

51. UK CAA. *CAP 562: Civil Aircraft Airworthiness Information and Procedures, Part 11 Leaflet 11-50*. UK Civil Aviation Authority, Gatwick.

52. UKCAA (2000). *Airworthiness Notice 71: Maintenance Error Management System (MEMS).* UK Civil Aviation Authority, Gatwick.

53. UK CAA (2007). *CAA Paper 2007/04 Aircraft Maintenance Incident Analysis. December* 2007. UK Civil Aviation Authority.

54. Rankin, W. L. (2000). The Maintenance Error Decision Aid (MEDA) Process. *Proceedings of the IEA 2000/HFES 2000 Congress.*

55. Boeing. *Maintenance Error decision Aid (MEDA) User Guide, at* http://www.atec.or.jp/SMS_WS_Boeing_MEDA%20Users%20Guide.pdfInternet (accessed 22 September 2010).

56. Bongard, J. A. (2001). Maintenance Error management through MEDA, *Proceedings of the 15th Annual Symposium – Human factors in Maintenance and Inspection, 27-29 March 2001,* London.

57. Vistair (2010). Airline Safety Management Systems. At http://web.vistair.com/solutions/airline-safety-management-systems/

58. AQD (2010). Integrated Safety and Risk Management System. 2010. AQD Superstructure: at http://www.superstructuregroup.com/aqd_isms.aspx.

59. Volpe (2005). *Highlights (news letter) Summer 2005*, The Volpe Centre at http://www.volpe.dot.gov Research and Innovation Technology Administration, National Transportation Systems Centre.

60. Setti, G. H. (2007). *SPAS: Safety Performance Analysis System. General Briefing FAA AFS-900,* August 2007. Federal Aviation Administration, Dulles, VA 20166.

61. GAO (1996). *Aviation Safety - Targeting and Training of FAA's Safety Inspector Workforce. GAO/T-RCED-96-26.* United States General Accounting Office (1996).

62. Terpstra, P. (2007). *Risk Analyses in CAA-NL (Airworthiness).* Proceedings of a Workshop at UK CAA on 11-12 September 2007, UK Civil Aviation Authority, Gatwick.

63. Shappell, S. A., Wiegmann, D.A. (2000). *The Human Factors Analysis and Classification System–HFACS. DOT/FAA/AM-00/7*, US Department of Transportation, Federal Aviation Administration, February 2000.

64. Watson, J., Kanski, B., *Human Factors Analysis and Classification System–Maintenance Extension (HFACS-ME). Student Guide V3.0.* US Naval Safety Centre, School of Aviation Safety.

65. EASA. *ECCAIRS Program.* At European Aviation Safety Agency web site http://www.easa.europa.eu/safety-and-research/ECCAIRS.php.

66. ICAO. ADREP 2000 Standard. International Civil Aviation Organization. At http://www.icao.int/anb/aig/Taxonomy/R4LDTopicsSectionsandAttributes.pdf.

67. Hale, A. (2002). Risk contours and risk management criteria for safety at major airports, with particular reference to the case of Schipol. *Safety Science* 40, pp 293-323.

68. Ale, B. (2002). Risk assessment practices in the Netherlands. *Safety Science 40*, pp 105-126.

69. Ale, B. J. M., and Piers, M. (2000). The assessment and management of third party risk around a major airport. National Aerospace, Netherlands. *Journal of Hazardous Materials,* Volume 71, Issues 1-3, 7 January 2000, Pages 1-16.

70. Netjasov, F., Janic, M. (2008). A review of research on risk and safety modelling in civil aviation. *Journal of Air transport Management* 14 (2008*)* pp 213-220.

71. Dalkey, N. C. (1969). *The Delphi Method: An Experimental Study of group Opinion. Report RM – 5888.* Rand corporation, June 1969.

72. Ford., D. A. (1975). Shang Inquiry as an Alternative to Delphi: Some Experimental Findings. *Technical Forecasting and Social Change,* 7, 139 -164 (1975).

73. Saaty, T. L. (1977). A Scaling Method for Priorities in Hierarchical Structures. *Journal of Mathematical Psychology*, 15, No 3, June 1977, pp 234 – 281.

74 Mukaidono, M. (2001*). Fuzzy Logic for Beginners*. World Scientific publishing 2001, Singapore.

75. Cox, E. (1998) *The Fuzzy Systems Handbook: A practitioner's guide to building, using, maintaining fuzzy systems*. Academic Press Professional. Boston.

76. Kaehler, S. D. (2010) Fuzzy Logic- An Introduction Part 1 www.searchseattlerobotics.org accessed on 10 December 2010.

77. McCarthy, J, Schwartz, D., Osborne, D. and Hadjimichael, M. (1999). Modeling risk with the Flight Operations Risk Assessment System (FORAS). In *Proceedings, International Air Safety Seminar, Rio de Janeiro, Brazil*. Flight Safety Foundation, Nov 1999.

78. Hamad, A. S. J. R. (2010). *Human Factors Effects in Helicopter Maintenance: Proactive Monitoring and Controlling Techniques.* Doctoral Thesis, Cranfield University, 2010.

79. Pearl, J. (2009). *Causality: Models, Reasoning and Inference.* Cambridge University Press, 2009.

80. Jensen, F. V. (1996). *Introduction to Bayesian Networks.* New York: Springer – Verlag, 1996.

81. Patankar, M.S. and Taylor, J.C. Posterior probabilities of causal factors leading to unairworthy dispatch after maintenance. *Journal of Quality in Maintenance Engineering*, Volume 9, No: 1, 2003, pp 38-47. Emerald.

82. Sahin, F., Yavuz, M. C., Arnavut, Z. and Uluyol, O. (2006). Fault diagnosis for airplane engines using Bayesian networks and distributed particle swarm optimization. Elsevier 2006.

83. Luxhøj, J. T. (2002). Risk analysis of human performance in aviation maintenance. *16th Human factors in aviation maintenance symposium, April 2.-4, 2002*.

84. Luxhoj, J. T (2003). *Probabilistic Causal Analysis for System Safety Risk Assessments in Commercial Air Transport*. Dept of Industrial and Systems Engineering, Rutgers University, 2003.

85. Clemen, R. T. (2000). *Making Hard Decisions – An Introduction to Decision Analysis,* Duxbury Press, 2000.

86. Reason, J. (1990). *Human Error.* Cambridge: Cambridge University Press, 1990.

87. Reason, J. (1997). *Managing the Risks of Organizational Accidents.* Ashgate Publishing, Aldershot, UK, 1997.

88. Bolstad, W. M. (2004). *Introduction to Bayesian Statistics*. Wiley-Inter Science, 2004.

89. Spiegelhalter, D. J., Dawid, D. J., Phillip, A., Lauritzen, S. L and Cowell, R. G. (1993). Bayesian Analysis in Expert Systems. *Statistical Science* Volume 8 No: 3, 219-247.

90. Norsys (2003). *NETICA User's Guide. Application for Belief Networks and Influence Diagrams. Version 1.06 for Windows*. Norsys Software Corporation, 2003.

91. Luxhøj, J.T., M. Jalil, and S.M. Jones (2003). A Risk- Based Decision Support Tool for Evaluating Aviation Technology Integration in the National Airspace System, *Proceedings of the AIAA's 3rd Annual Aviation Technology, Integration, and Operations (ATIO) Technical Forum*, Denver, Colorado, November 17-19.

92. Yin, Robert K. *Case Study Research – Design and methods*, 4th Ed, Sage, 2009

93. Rasmussen, J. (1997). Risk management in a Dynamic Society: A Modelling Problem, *Safety Science*, Volume 27, No. 2/3, pp 181-213, 1997.

94. DFT (2003). *Report of the inter-departmental working group on the training of aircraft maintenance engineers, paragraphs 82-83*, Department for Transport, London, 2003.

95. Ale, B.J.M., Bellamy, L. J., Cooke, R.M., Goossens, L.H.J., Hale, A.R., Kurowicks, D., Roelen, A.L.C. and E. Smith (2005). "Development of a Causal Model for Air Transport Safety, *Proceedings of the European Safety and Reliability Conference*, Gdansk, Poland, pp. 37-44.

96. MoD (UK). Organization and Policy Leaflet 315, Structural Integrity of RAF Aircraft. *AP 100A-01 Royal Air Force Engineering.*

97. EASA. *Regulation 1702/2003 Part 21.* European Aviation Safety Agency.

98. EASA. *Regulation 2042/2003 Part M and Part 145, Part 66 and Part 147*. European Aviation Safety Agency.

99. Phillips L.D. (1984). A Theory of Requisite Decision Models. *Acta Psychologica*, 56, 29-48.

100. Neapolitan, 1R. E. (1990). *Probabilistic Reasoning in Expert Systems.* John Wiley & Sons, Inc, New York, 1990.

101. Pearl, J. (1991). *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann, San Mateco, CA. 2nd edition 1991.

102. Haddon-Cave, C. (2009). *The Nimrod review. An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV 230 in Afghanistan in 2006*, London: The Stationery Office 2009.

103. Fenton, N. (2010). *Probability Theory and Bayesian Belief Bayesian Networks*, at http://www.eecs.qmul.ac.uk/~norman/BBNs/BBNs.htm (accessed 13 November 2010).

104. GAO (2009). Better Data and Targeted FAA Efforts Needed to Identify and Address Safety Issues of Small Air cargo Carriers – GAO-09-614, US Government Accountability Office. Aviation Safety. June 2009.

105. UK CAA. CAA Paper 2009/05 Aircraft Maintenance Incident Analysis. July 2009. UK Civil Aviation Authority.

106. UK CAA. *Safety Regulation Group: Safety management Systems – Guidance to Organizations*. July 2010. UK Civil Aviation Authority.

107. CHIRP/MEMS database at http://www.chirp-mems.co.uk/CHIRP-MEMS%20data%20review_files/frame.htm

108. CIAIAC (2008). *Accident Involving aircraft McDonald Douglas DC-9-82 (MD-82) Registration EC-HFP, operated by Spanair, at Madrid – Barajas airport on 20 August 2008. Interim Report of A-032/2008*. Commission for the Investigation of Civil Aviation Incidents (CIAIAC) of Spain.

109. UK CAA. CAP 776. Global Fatal Accident Review. 1997 – 2006. UK Civil Aviation Authority.

110. Frackowiak, R.S.J. (2004). *Human Brain Function*. 2nd Ed. Academic Press, London.

111. RCPsych. *Fact Sheet on Depression*. Royal College of Psychiatrists.

112. Jauregui, F., Hosey, P. (2005). Extended Work Hours (Maintenance). February 2005. International Federation of Airworthiness

113. Carroll, B. (1999). Irregularities in airline safety checks under Govt investigations. *The Examiner, Irish News*, 22 May 1999.

114. IATA Press Release No: 10. 23 February 2011. Accessed on 14 June 2011 at http://www.iata.org/pressroom/pr/Pages/2011-02-23-01.aspx

115. Sarsfield, L. P., Stanley, W. L., Leboa, C. C., Ettedgui, E., Honning, G. (2000). Safety in the Skies, Personnel and Parties in NTSB Aviation Accidents Investigation – Master Volume. Rand Institute of Civil Justice.

116. BTRE Report 113. Cost of Aviation Accidents and Incidents. Australian Government. Department of Transport and Regional Services, February 2006.

117. CHIRP/MEMS. Review of Installation Error. November 2007. http://www.chirp-mems.co.uk/CHIRP-MEMS%20data%20review_files/frame.htm

118. Hosey, P., Jauregui, F. Errors and the Influence of Working Patterns and Fatigue. IASS 2008. International Federation of Airworthiness.

Intentionally Blank

List of software files

The following software files are included in the accompanying CD/DVD, segregated into folders. They are listed here in the order as they appear in the CD/DVD.

L1	L2	L3	L4	L5	Remark
CD/DVD – Bayesian Model for Strategic Level Risk Assessment in CAW of Air Transport - Software					
	Integrated Model				Folder
		Combi5_All_Ver2 text file			Text
		Combi 5_All_Cer2_data for txt file			Excel
		DJ CAW Risk Model_Combi 5_All_Ver2			BBN
		DJ CAW Risk Model_Combi 5_All_Ver2_Air Cargo Subset			BBN
	Ops X Validation				Folder
		Ops X Base			Folder
			Ops X Base Yr 08_09_10		Folder
				DJ CAW Risk Model Ops X Base_Yr 08_09_10 Results	BBN
				Ops X Base Yr 08_09_10_date_for txt file	Excel
				Ops X Base Yr 08_09_10_text file	Text
			Ops X Base_Yr 08		Folder
				DJ CAW Risk Model Ops X Base Yr 08 Results	BBN
				Ops X base Yr 08 data_for txt file	Excel
				Ops X Base Yr 08_text file	Text
			Ops X Base_Yr 09_10		Folder
				DJ CAW Risk Model Ops X Base Yr 09_10 Results	BBN
				Ops X base Yr 09_10 data_for txt file	Excel
				Ops X Base Yr 09_10_text file	Text
		Ops X Operations			Folder
			Ops X Belief		Folder
				DJ CAW Risk Model for 1M Sectors_inc 600 error lines UK Stnd only	BBN
				DJ CAW Risk Model for 2M Sectors_inc 1200 error lines UK Stnd only	BBN
				DJ CAW Risk Model for 3M Sectors_inc 1800 error lines UK Stnd only	BBN
				DJ CAW Risk Model for 3M Sectors_inc 1800 error lines UK Stnd plus 34338 sec	BBN
				DJ CAW Risk Model for 6M Sectors_inc 3600 error lines UK Stnd only	BBN
				Modified Uk Stndard Case File V2 for txt	Excel
				Modified UK Stndard Case File V2 text file	Text
			Ops X Combine Years		Folder
				DJ CAW Risk Model Ops X Combie Years Risk Status_Yr 08_09_10 Result	BBN
				Ops X Error Data Combined Years_for txt file	Excel
				Ops X Error Data Combined Years_text file	Text
			Ops X Year 08		Folder
				DJ CAW Risk Model Ops X_Yr 08 Result	BBN
				Ops X Yr 08 data_for txt file	Excel
				Ops X Yr 08_text file	Text

L1	L2	L3	L4	L5	Remark
			Ops X Year 09_10		Folder
				DJ CAW Risk Model Ops X yr 09_10 Result	BBN
				Ops X Yr 09_10 data for txt file	Excel
				Ops X yr 09_10_text file	Text
	Subsystem Tests				Folder
		Change Management			Folder
			Change Manage_Datasheet_MSO_07		Excel
			Change Manage-Text File		Text
			DJ Change Management		BBN
		Compliance			Folder
			Compliance_Modified 120609 Data MSO_07		Excel
			Compliance_Modified Txt File		Text
			DJ Compliance_Pt145_PtM_TestV5_Modified 120609		BBN
		Consequences			Folder
			Consequence_Datasheet_Casefiles_Txt Word		Text
			Consequences_Datasheet_Casefiles_MSO_07		Excel
			Consequences_Datasheet_Casefiles_Txt file		Text
			DJ Consequence Loop		BBN
		Operation and Capability			Folder
			DJ Operation and Capability_V2		BBN
			Operation Capability_txt file		Text
			OpsVCapability_Datasheet_Casefile_MSO-07		Excel
		Pt145_Pt147 parts of Performance			Folder
			DJ Pt145_Pt147 Parts of Performance		BBN
			Pt145_Error_Datasheet_SRG Modif txt file		Text
			Pt145_Pt147_Casefile_MS07		Excel
		PtM_Pt21 parts of Performance			Folder
			Final Test Folder_Peformance Subsystem_PtMandPt21		Folder
				DJ Combine PtM_Pt145_Pt21 Interface_Performance	BBN
			DJ Part 21 TC		BBN
			Pt21_PtM Errors Case Files_txt_Word		Text
			Pt21_RegErr_Datafile		Excel
			Pt21_RegErr_Datafile_txt file		Text
		QA Sytem			Folder
			DJ Quality Audit		BBN
			QMS_Datasheet_Casefile_MS07		Excel
			QMS_Datasheet_txt file		Text

NOTE:

To view and interact with BBN files a NETICA v411, or later version, software program should be installed in the computer. It is not included in the CD/DVD due to licensing regulations.

Excel files will require MS Office 2007.

List of Appendices

Intentionally Blank

Appendix 1

Air transport industry consulted during the research program

A1.1 Organizations

- European Aviation Safety Agency, Safety and Research Department
- UK Civil Aviation Authority, Safety Regulation Group
- UK Civil Aviation Authority, Economic Regulation Group (Departments for Legal, Insurance and Fleet Usage Statistics)
- UK Flight Safety Committee (FSC)
- UK FSC Maintenance Sub Committee
- International Federation of Airworthiness Engineers
- MoD RAF - former Directorate of Aviation Regulation & Safety
- Confidential Human Factors Incident Reporting Programme – Maintenance Error Management System (CHIRP/MEMS)
- Baines Simmons international
- International Bureau of Aviation, IBA Group
- Association of Licensed Aircraft Engineers (ALAE)
- Large long haul air line 1
- Large long haul airline 2
- Regional airline
- Regional air line - Engineering Services/ MRO
- Large air cargo operator 1
- Large air cargo operator 2
- Business jet operator
- Business jet operator maintenance dept/ MRO
- Large aircraft MRO

A1.2 Courses / Seminars/ Workshops / Conferences Attended

- Decision Analysis Course – Defence College of Management & Technology, Shrivenham - 2008
- Advances in Risk & Reliability Technology Symposium - 18th AR2TS – Loughborough University - 2009
- Risk Analyses Model - Civil Aviation Agency of The Netherlands – 2007
- Basic Human Factors Course – CAA International - 2007
- Advanced Human Factors – CAA International – 2008
- Human factors Conference - Royal Aeronautical Society –2009

- Part 145 EASA Regulation – CAA International - 2007
- Part M EASA Regulation – CAA International - 2007
- Airworthiness & Maintenance Conference – Royal Aeronautical Society – 2008
- Airworthiness Management – IBA Group – 2009
- UK FSC and UK FSC MSC 2-monthly meetings – 2008 to 2010
- 62nd Annual International Air safety Seminar – Flight Safety Foundation - 2009
- Future MRO in Civil Aviation – 2008
- Future MRO in Civil Aviation – 2009
- Military Aircraft Maintenance & Repair – 2010
- Maintenance, repair & Overhaul (MRO) Oversight Today and The Future – Federal Aviation Administration - 2010
- Aviation Disaster: Investigating the Causes, Resolving the Claims – Avicon/ RTi/IMC/ Cozen/ INCE - 2008

Appendix 2

Specimen case studies - Accidents resulting from human error

A2.1 Case 1 – Errors in maintenance practices and aircraft maintenance manual[4]

On Thursday 10th Jun 2004 at 19:07 UTC a British Airways Boeing 777 G-YMME, carrying 151 passengers and a flight crew of 15 took off from London Heathrow bound for Harare, Zimbabwe. Unknown to the Captain, the aircraft was spilling large quantities of fuel as it was rotating for take-off, but the captain of another aircraft that was waiting for take-off clearance witnessed the event and reported to Heathrow air traffic control. By this time G-YMME was climbing away trailing a 2-mile long plume of escaping fuel, putting the aircraft in danger from fire and explosion.

Heathrow ATC promptly alerted the captain of G-YMME, who confirmed the fuel loss and decided to recover his aircraft back to Heathrow. He jettisoned part of his fuel load over the sea to make his aircraft light enough to land, and recovered back to Heathrow uneventfully.

Soon after landing and once the aircraft came to rest, emergency crews inspected the aircraft and confirmed the strong presence of fuel vapor in the port landing gear bay area. The port engine was shut off, the aircraft taxied back to the terminal where the passengers were disembarked.

Further inspection of the aircraft on the ramp revealed that fuel had spilled out of the aircraft's centre wing area tank (CWT), from an open aperture known as a purge door. The open purge door-panel was found hanging on a lanyard inside the tank. Hanging beside the open aperture, there was a transparent plastic bag secured to the tank structure with a string, which contained the screw fasteners for the door and some escaped fuel.

This incident was at the centre of a UK Aircraft Accident Investigation Board (UK AAIB) enquiry which revealed that the purge door had been opened during a scheduled base maintenance inspection of the aircraft, which had been completed about one month before this accident. Unknowing to those authorize to release the aircraft, it had been released to service with an incomplete maintenance task, i.e. with the door still open. Following release to service, the aircraft had flown several sectors over a period of one-month, carrying the dormant error. Unfortunately, because of the relatively small fuel load that had been carried in the CWT in those flights, the error had not come to

anyone's notice. However, for the Harare bound flight, a larger fuel load had been carried, which on this occasion spilled out of the tank as the aircraft was taking off.

Figure 2 - Purge door opening. Fuel and retaining screws inside plastic bag. Purge door is hanging on lanyard inside the fuel tank. The O-ring seal was removed from the purge door by maintenance staff following the incident.

Figure A2.1 – Open Fuel Tank Purge Door – Source of fuel spillage (Source: UK AAIB)

The presence of an open purge door and the failure to detect it was due to a catalogue of errors committed by the engineers involved, as well as the managers who were supervising and coordinating the maintenance tasks. During the investigation, the Board discovered further errors in the technical documentation associated with the tank purging, leak testing and structural inspection of the tank. There were also failures by the maintenance organization to account for the people who worked on the aircraft, as well as to mal practices of utilizing personnel unqualified on the type for supplementary work. These errors were as follows:

- According to the AMM for B-777 aircraft, purge door removal was not an authorized procedure for the task. A person employed on the aircraft had removed it because of his prior experience on B-747 aircraft that had a similar

purge door in the centre wing tank (CWT), or if not he had instructed another person to remove it. This was the initial error, because he was using an unauthorized procedure.

- The removal would have been acceptable, had it been reported and a job card was raised. This had not been done, and therefore the failure to raise a job card to register the deviation from AMM constituted the primary error.

- This primary error had given rise to the following consequences that compounded the original error.
    - Proper coordination of the task completion, supervision and inspection of the area had not been carried out, as none of the engineers and managers tasked with this work was aware that a purge door had been removed.
    - A purge door removal job card, had it been raised, would have cross referred to the purge door leak test. Since there was no job card, there was no cross-reference, i.e. no work record trail.
    - A general catch-all leak test had been done to cover all known engineering tasks on the CWT. A 40,000 kg fuel load, believed to be an adequate amount, had been used but this amount was insufficient to cover the purge door. It has since been established by the investigators that to catch a purge door leak an uplift of 52,200 kg was needed. The limited catch-all leak test failed to detect the open purge door.
    - Investigation also revealed that the published information in AMM on the purge door leak test was erratic, in that it called for a test using 32,000 kg, whereas the correct amount should be 52,163 kg. Misinformation in the AMM was a dormant error, though in this case it had not contributed to the error.

- As a spin-off of the investigation, it has been discovered that the AMM was at error in referring to the structural area that needed inspection, for which the tank was drained and ventilated. The area within the tank that needed inspection was in fact quite different from the area illustrated on the AMM. It follows therefore, that all previous inspections that had been carried out on this aircraft and others might not have met the intended purpose. AAIB report had not dwelled on the way how BA recovered from any past errors. However, for the future, the AMM has been amended to provide accurate information.

- Access to the CWT and follow up inspection procedure required the removal of a baffle door. This information had not been mentioned in the AMM. That means the AMM had been in error, and in the past, engineers might well have deviated from AMM procedures whilst undertaking this task. AMM has been amended since this discovery.

- There had been no record of the persons who were involved in the tank inspection of repair; therefore there was no means of identifying the person involved in the error. The maintenance organization had been moving labor between different types of aircraft regardless of the fact that some might not have the correct rating for the aircraft on which they were deployed, e.g. using a B-747 rated engineer on a B-777 aircraft. Nor have the management kept track of their deployment. AAIB report identified the issues concerned but has stopped short of commenting of internal labor management arrangements that might have contributed to this error.

- None of the ground inspections of the aircraft during the one-month period detected the open door. Clearly this suggests that pre-flight inspections were probably too focused and the general surveillance of the state of the aircraft was superficial. In mitigation it has been said that the purge door opening was at a high up location, inside the port wheel well, which is not easily visible from ground.

Luckily there was no fire and explosion on this occasion, even though the possibility existed as there were heat sources in the vicinity.

A2.2 Case 2 – Design, Changes to Operating patterns and Change Management[10]

On 17th January 2008 a British Airways Boeing 777-236ER G-YMMM, inbound from Beijing China, was coming into land at Heathrow airport. As the aircraft was at the final phase of the approach, its Rolls Royce Trent engines began to lose power and failed to respond to critical power demands. Eventually, with the engines rotating just above the idling speed, the aircraft managed to glide into the airfield, crash landing on the grass area short of the runway threshold. With skilful handling of the aircraft at this critical stage, the pilot averted a potential disaster that could have resulted from the aircraft crashing into the thickly populated, built up area surrounding the airport. One passenger suffered serious injury during the crash landing; 34 passengers and 13 crew members suffered minor injuries; the remainder of the 135 passengers and 16 flight crew members escaped unhurt.

There was strong suspicion from the outset that the power loss might have been due to fuel starvation to the engines. But two more years of investigation had to pass by before UK AAIB concluded that it was ice accretion and blockage of the fuel-oil heat exchanger in the fuel flow path to the engine that had caused the starvation. AAIB Report[10] summarizes its findings as follows:

"Whilst on approach to London (Heathrow) from Beijing, China, at 720 feet AGL, the right engine of G-YMMM ceased responding to auto throttle commands for increased power and instead the power reduced to 1.03 Engine Pressure Ratio (EPR). Seven seconds later the left engine power reduced to 1.02 EPR. This reduction led to a loss of airspeed and the aircraft touching down some 330 m short of the paved surface of Runway 27L at London Heathrow. The investigation identified that the reduction in thrust was due to restricted fuel flow to both engines.

It was determined that this restriction occurred on the right engine at its Fuel Oil Heat Exchanger (FOHE). For the left engine, the investigation concluded that the restriction most likely occurred at its FOHE. However, due to limitations in available recorded data, it was not possible totally to eliminate the possibility of a restriction elsewhere in the fuel system, although the testing and data mining activity carried out for this investigation suggested that this was very unlikely. Further, the likelihood of a separate restriction mechanism occurring within seven seconds of that for the right engine was determined to be very low.

The investigation identified the following probable causal factors that led to the fuel flow restrictions:

1) Accreted ice from within the fuel system [1] released, causing a restriction to the engine fuel flow at the face of the FOHE, on both of the engines.

2) Ice had formed within the fuel system, from water that occurred naturally in the fuel, whilst the aircraft operated with low fuel flows over a long period and the localized fuel temperatures were in an area described as the 'sticky range'.

3) The FOHE, although compliant with the applicable certification requirements, was shown to be susceptible to restriction when presented with soft ice in a high concentration, with a fuel temperature that is below -10°C and a fuel flow above flight idle.

4) Certification requirements, with which the aircraft and engine fuel systems had to comply, did not take account of this phenomenon as the risk was unrecognized at that time".

[1] Fuel system upstream of FOHE.

At the Flight Safety Foundation's 62nd International Air Safety Seminar, 2009, a Boeing representative presented detail findings of a technical investigation into the fuel-oil heat exchanger design. It has been established during the investigation that some other versions of Boeing 777 aircraft have GE engines in which the heat exchanger was from a different supplier. Although those versions had flown similar long-transit polar routes, they have had no previous heat exchanger icing incidents reported. In fact there was a detail design difference between the two types of heat exchangers, which might explain why the RR engines heat exchanger was likely to be susceptible to ice accretion.

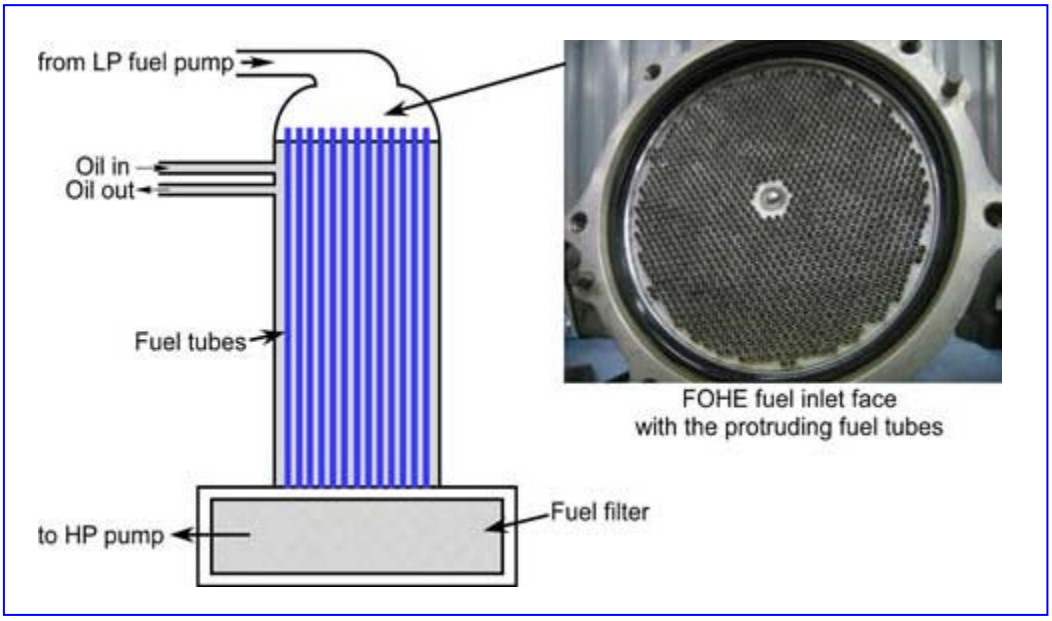


Figure A2.2 – Fuel-Oil Heat Exchanger – Location of ice accretion (Source: UK AAIB)

The GE engine's version had a smooth surface on the fuel inlet side of the heat exchanger matrix, whereas the RR engine version had a rough inlet surface where the tubes of the matrix were protruding through the surface. It seems that this detail difference of protrusions was critical as it was contributory to trapping the ice particles that were floating in fuel, before they enter the tubes where the particles would have been melted. This phenomenon is similar to autumn leaves accumulating near those parts of buildings where the wind flow is stagnant. Here, a lesson from nature would have taught the heat exchanger designers a lesson had they been mindful.

This then is an example of a design shortfall, due to limitation of knowledge, which in turn limited the scope of design and reliability testing specifications for this component. The conditions might have been exacerbated by the Boeing 777 aircraft's increased utilization in polar routes, which would increase the probability of encountering unusual cold conditions than that had been previously perceived. All these conditions would go into reliability testing but in this case, certification had proceeded on the basis of known information. It seems that at the time, all stake holders had missed to notice the detail differences in the design of two types of heat exchangers and to ask the question, why were they different?

This case is also an example to demonstrate change management, in this case the need for strict discipline in managing detailed technical investigations required before the role and utilization of an aircraft is changed from the specification for which it was initially designed. There is no evidence to suggest that management did not take place; the situation is highlighted to underscore the importance of change management. The end result is adequate evidence to indicate if that management process had been sufficient or not, and if decisions to fly polar routes were swayed by commercial sense despite unknown risk influencing factors coming from equipment limitations.

A2.3 Case 3 – Maintenance, Airfield Management, Design[9]

Both the previous cases ended up with no fatalities. But the case of Air France Concorde Flight Number 4590 that departed from Paris Charles de Gaulle airport ended up tragically. All occupants perished when the aircraft caught fire during take-off and then lost its capability to maintain speed and height until it could be safely recovered to an adjacent airfield. The aircraft crashed into a hotel at Gonesse, near Le Bourget' air field, in the conurbation of Paris, north. All the 109 occupants on board died along with 4 people on the ground. Six others on the ground were injured.

Figure A2.3 – Concorde Flight 4590 – Damaged by debris from a burst tyre
(Source: amazingdata.com)

During the take-off run, the aircraft had run over a loose metal strip that had fallen on to the run way from a Continental Airlines, DC-10, that had previously used the runway. The edge of the metal strip had cut into one of the Concorde's tyres, bursting them and then parts of debris from the explosion impacting on the under surface of the wing and so piercing an integral fuel tank located in the impact area. Fuel spilt under surge pressure and high speed conditions had caught fire from the engine afterburners. Subsequently, investigators had traced the source of the metal strip to a thrust reverser of the DC-10, which had been repaired to a poor standard, in that the security of the metal strip had not been assure, and the specified material stainless-steel had been substituted with titanium.

It is noteworthy that there have been more than 50 several prior cases of burst tyre some of which ended up with damaged fuel tanks and potentially serious consequences. Ironically the authorities, including the airlines involved, had not followed up the investigations to a positive conclusion and a lasting solution, leaving the aircraft vulnerable to similar repetitive hazards.

Figure A2.4 – Causal factor _ Runway debris (titanium metal strip)
(Source: BEA Report[9])

The French investigation report into the accident, also found, that a scheduled runway sweep for debris, which had been timed to take place prior to Concorde's departure, had been postponed to a much later time because of an exercise.

Figure A2.5 – Fragments of the burst tyre found on runway
(Source: BEA Report[9])

On the 6th December 2010, a French Court passed its judgment on the crash, apportioning part of the blame to Continental Airlines and the engineer who performed the maintenance activity on the metal strip. It also passed on the blame to the consortium who designed and manufactured the aircraft, now trading under the name EADS, for failing to act decisively to find a design solution to the consequences of high speed tyre bursts, many of which Concorde experienced during its service life.

The issue of runway sweep had not been cited in the final verdict.

A2.4 Case 4 – Old cargo aircraft. Continuing Airworthiness. Inspection Schedules[24]

Finally another case is narrated here briefly, this one regarding the cargo aircraft El Al Flight 1862, Boeing 747-258F 4X-AXG that crashed on to an apartment building at Bijlmermeer, Amsterdam on taking off from Schipol airport on 4th October 1992.

The aircraft has just taken off from Schipol airport with a cargo load of 60 tons and one passenger, and was climbing through FL 60. During the climb, Number 3 engine got detached from the wing, which in turn hit Number 4 engine and tore that off the aircraft. With two engines lost from the same side and, now, the aircraft highly unstable, the pilot tried to recover it back to Schipol airport. But in the process, he gradually lost control of the aircraft. It eventually hit a block of flats at a near 90-degree bank angle and crashed. All on board (4) and a number of residents (43) died and there were many other casualties of varying degrees of seriousness.

Figure A2.3 – Simulation of the end of El AL Flight 1862
(Source: aviationknowledge.wikidot.com)

Investigations revealed the following. In case of an accidental separation of an engine, there was a fuse pin that usually cleanly separates the engine from its pylon. In this case, the fuse pin did not function properly because it was the fuse pin itself that had fractured through a fatigue crack that developed in the fuse pin.

The aircraft was 13-years old at the time. The aircraft had completed 257 flight cycles since the mid spar fuse pin, this being the source of the fatigue crack, was last inspected under the applicable service bulletins and airworthiness directives.

Continuing airworthiness assurance programs for this aircraft, in terms of inspections and NDT examinations, had been found to be inadequate to detect the crack.

The investigation boards conclusion[24] was that the *"design and certification of the B747 pylon was found to be inadequate to provide the required level of safety. Furthermore the system to ensure structural integrity by inspection had failed. This ultimately caused – probably initiated by fatigue in the inboard mid-spar fuse pin – the No 3 pylon and engine to separate from the wing in such a way that the No 4 pylon and engine was torn off, part of the leading edge of the wing was damaged, and the use of several systems was lost or limited".*

The case of the El Al cargo flight is complex, in that the error of judgment on the adequacy of inspection lay in the domain of initial certification, which probably had not been revisited to review if the assumption made at the time were still valid in the light of experience with the aircraft in operational service as a cargo aircraft.

Therefore, one could argue that this falls into the domain of continuing airworthiness, where an aircraft ageing process, susceptibility to fatigue and adequacy of inspection procedure to meet the intended purpose ought to be reviewed in a continuing review process.

Figure A2.4 – Similar location of the engine pylon fuse pin
(Source: airliners.net)

This then is a human failure at a higher, intellectual level where fleet managers operate, and where there ought to be continuing dialogue with the Design Authorities.

This particular case underscores the vulnerability of older aircraft often used either in the cargo role or in some low cost airlines or in countries where airlines are run on meager budgets.

The aircraft crashing into a block of flats, and the subsequent fears of it having released radioactive materials to the environment was a highly controversial issue at the time. It was also claimed that by media that certain toxic chemicals for military use might have been carried in the aircraft[25.]

It has raised fears amongst local authorities in populous conurbations over the specter of cargo aircraft operating from their airports, often in silent hours when people are asleep in their homes, thus making the environment very vulnerable to aircraft crashes. They feared for the safety of their citizens and fixed assets on the ground, and more importantly the long term health and safety issues arising from dangerous substances that might be released to the environment.

A2.5 Case 5 – Time pressure, old aircraft, low cost airlines[108]

On 20 August 2008, a Spanair Boeing MD-82 aircraft, Flight JF5022 to Gran Canaria, carrying 172 occupants was taking off from Madrid airport, when it failed to reach height, went out of control and crashed just outside the airfield. Only 18 occupants survived the crash.

The final report of the accident investigation by Commission for the Investigation of Civil Aviation Incidents (CIAIAC) of Spain was due publication in December 2010. Meanwhile, following information from CIAIAC interim report points to possible human error, both in flight operations and CAW processes, combined with possible equipment failure. This is an example of a system failure that has brought tragic consequences.

Accident investigations so far has revealed that the flap position had not been in the correct configuration prior to takeoff, and that the flight crew had missed noticing its abnormal position during takeoff. Evidence from Digital Flight Data Recording System (DFDRS) confirms that the flaps and slats had been fully retracted; the takeoff warning system had not been activated.

The reason for the failure of flight crew to detect an abnormal flap configuration is still under investigation. One contributory factor to the situation was thought to be the failure of flap position warning system to operate.

It has been reported that this flight has had one previous departure attempt abandoned, when the pilot returned the aircraft to the gate due to abnormal temperature indications from the Ram Air Temperature (RAT) probe. It is understood that in rectifying the problem, an engineer had deactivated the RAT probe's heating circuit by dismantling the Z-29 circuit breaker.

CB Z-29 also supplies power to the Thrust Rating Indicator (TRI) Panel in the cockpit, which is part of the Thrust Rating System (TRS). Without AC power the panel will be inoperative and the TRS will not be available; moreover, the auto-throttle will not receive signal from TRP, and so, the Engine Power rating (EPR) setting would have to be set manually (Section 1.2.5 of the Interim Report). DDRS data (Section 1.3.2) confirm that engine power settings had to be manually set during takeoff.

Dismantled Z-29 alone does not answer the issue of inactive TOWS. This receives power from R2-5 Relay that is operated by undercarriage nose strut when on the ground. The same relay disconnects power supply to the RAT probe heating element, when the aircraft is on ground.

Investigation into past cases of R2-5 failures, some which had been intermittent failures, indicate that they have resulted with either TOWS failures or RAT probe heating on the ground (Section 1.2.4 and Section 2.2 of the Interim Report).

Although the accident investigation could not find conclusive evidence of R2-5 failure in the Relay recovered from the crashed aircraft, other simulated tests done on same type of Relay fitted to another aircraft of the same MD family, has confirmed that if there was a complete failure of power supply to the R2-5 Relay, or a break in K-33 CB that supplies power to some parts of R2-5 Relay, then it is possible for TOWS malfunction as well as RAT probe overheating (Section 1.4.4).

There are no indications in the interim report if CB K-33 was removed during rectification of defect on RAT probe. CB K-33 was located in the top panel, behind the LH seat in the cockpit, and the Z-29 in the lower panel, behind LH seat, i.e. in close proximity.

It was also noted that from DFDRS data, that the flap position had indicated 11 degrees until the time the aircraft returned to the gate for RAT probe defect rectification. However it had been recording Zero (0) degree position from the time it left the gate after rectification, until the time the aircraft crashed [Section 1.3.2). This suggests that, either the flap was not reset before leaving the gate the second time. There are indications from DFDRS data that the flight crew was anxious of the delay caused by the defect, and that check list procedures were not being strictly adhered to, i.e. anticipating check list steps, not responding to them mindfully, and being distracted by other actions.

In order for TOWS not to work during takeoff, with a wrong configuration, either CB K-33 should have been dismantled, or there ought to be an internal contact failure within the relay, that supplied power to the TOWS. DFDRS data confirm that there had been no sound from TOWS during takeoff run, indicating that there was no power supply to TOWS. This could be due to a faulty internal contact within the relay, or if not power supply failure to the relevant contact in the Relay, by way of an open CB K-33.

The interim report is inconclusive as to why TOWS was inoperative, which could either be due to removal of K-33 CB or an internal fault of R2-5 Relay.

Further tests on the equipment and investigation of human factor issues were to be undertaken prior to the issue of the final report in December 2010.

It would be interesting to see if working under time pressure had contributed to a misdiagnosis of R2-5 Relay during maintenance, or if K-33 CB was dismantled as part of isolating the RAT probe heater circuit or as a diagnostic check, but had forgotten to be re-assembled. The close location of the two CBs also of interest, where a human error could be made, and gone unnoticed, when under pressure.

Spanair is a low cost airline; MD-82 is a relatively aged aircraft with older generation technology.

Appendix 3

Rationale for the high-level influence diagram

A3.1. Constituents of the Influence Diagram

For analytical purposes, it was necessary to make CAW process stand alone, and that had been achieved by assuming that all other regulated processes involved in launching and delivering a safe flight, namely, flight operations, air traffic control and airfield operations have remained error- free.

Thus the exploratory ID (which incidentally was in a draft form) represented the synergy of various groups and organizations, and their activities, in an integrated CAW process network in isolation.

All the participants to the CAW process could be pooled as “core groups” and “peripheral groups” according to their respective, direct or indirect involvement with the end product.

Between Type Certification of an aircraft and its commercial operation, there existed an integrated logistic support system (ILS) and a complex organizational and management infrastructure, required to uphold the CAW process. Errors can occur anywhere in that entire complex dynamic system.

Part of this infrastructure lay within the core group, but part lay outside the core, amongst the peripheral groups.

A3.2 Core group and error contributions

The core groups that directly contributed to the generation of the end product were the combined group of “continuing airworthiness management organization of an air operator” its “line maintenance organization” (i.e. Part M and Part 145 approved organizations) together with their “corporate business management organization”. The airworthiness management and maintenance group undertook CAW management, engineering operations and flight handling. The business group took on financial and legal responsibilities for the end product as well as benefitting from the revenue generated from them, namely the “revenue generating flights”.

The objective of the core groups was to deliver a safe non-risk flight. However, despite the best of intentions, that objective might not always be realized because of human error or other organizational and system shortfalls in the CAW process. Thus a flight could experience an incident of varying severity or, if not, it might not even be launched or delivered on time as scheduled.

A3.3 Peripheral groups and error contributions

Peripheral groups that supported and influenced the core group's CAW activities were other regulated approved organizations (AO), namely:

- Maintenance, Repair and Overhaul Organizations (MRO), i.e., Part 145 Approved Organizations (AO).
- Design Manufacturing and Production Organizations, Part 21 AO.
- Training organizations, i.e. Part 147 AO.

A3.3.1 Part 145 AO

Part 145 AO, apart from providing line maintenance services also undertook off-line base servicing support, deep repairs and component overhaul services.

A3.3.2 Part 21 AO

Parts 21 AO were usually the aircraft and component Design Authorities (DA), Original Equipment Manufacturers (OEM) and those who produce parts under parts manufacturer approval (PMA). In CAW, Part 21 AO provided Post Design Services (PDS) relating to their products. Some of the causal factors that directly gave rise to unsafe incidents or if not contributed to error at human/.machine interface have had their roots in Part 21 organizations, e.g. errors or shortfalls in design, manufacture or integrated logistic support (ILS) elements, or their planning and related upstream processes.

A3.3.3 Supply chain

In CAW process, supply chain organizations ensured a flow of regulated materiel, e.g. components and spare parts, from Part 21 AO to Part 145 AO. It was known that other unregulated supply chains also existed in aviation industry.

Although OEM and PMA parts were well regulated, reports had pointed to “rogue parts” entering supply chains, which suggested the abuse of supply chains despite material entry and exit points of AO were controlled as per regulation.

A3.3.4 Part 147 AO

Part 147 approved training organizations were another peripheral group; they were responsible for the formation and qualification of technical personnel employed in CAW process. Despite apparently meticulous compliance with the training and qualification processes for personnel, it was the very same engineers that these AO turn out who made mistakes at the work place.

Mentioned amongst the many contributory factors at personal level, which related to error, were shortfalls in training. These shortfalls had been recognized as poor quality and training standards, and shortfalls in the wider technical knowledge that was needed to supplement the ever more increasing focussed training.

There was a general recognition within the industry that the modern training environment and techniques, more based on economising in training and minimising knowledge transfer, were being run on commercial basis. That meant, meeting the minimum standards acceptable in industry. In contrast, there is a belief amongst experienced and time served engineers and managers in the industry that modern training establishments do not produce the same type of high quality practical engineer as that used to be produced by traditional apprentice training. Supporting this argument, literature had pointed out that shortfall in standards in newly recruited engineers, though it is strictly not an error, would lead to individual personnel error during the performance of engineering activities or in exercising judgement under pressure conditions.

A3.3.5 Rule maker/ Regulator

The exploratory ID recognized the roles of the Rule Maker and/or Regulator. The former made and issued the rules and the latter exercised a supervisory role over their compliance by approved organizations. For civil aviation in the UK, EASA was the rule making body whereas the UK Civil Aviation Authority was the national competent authority or Regulator for short. Both these establishments function in harmony with ICAO that guides nations on international air safety standards on behalf of the United Nations.

The roles and authority alone of these regulatory bodies do not make them immune to errors since personnel manning these organizations, are just as fallible as the engineers and managers who worked in the aviation industry. There had been reports of either regulation themselves had been faulty or erratic, or if not the officials themselves had contributed to human error whilst managing rules. Such events could be considered as failures of the very defences themselves, though mercifully, they do not happen often.

Error contribution from such authorities would be relevant to this study, and it was envisaged that appropriate high level input in the form of error data would be forthcoming.

A3.3.6 Global influences

Global influences had been identified in the ID, and were meant to cover wider issues that affected all air operators and supporting approved organizations. Such wider issues included, e.g., global economic fluctuations, fuel prices, technology changes, open sky policies, major trends in public behaviour relating to air travel. This was not an exhaustive list.

A3.3.7 ICAO

ICAO, though an important global player, was not specifically identified in the ID. However, any binding agreements, advice or mandates that ICAO had issued could be considered as part of the global influences that affected the aviation business. ICAO mandate on Safety Management Systems was a case in point. It was assumed that any mandatory influences originating from ICAO had been passed down to AO through Regulator.

A3.3.8 IATA and TIACA

International Air Transport Association (IATA) and The International Air Cargo Association (TIACA) respectively were global, commercially centred organizations that influenced the way commercial aircraft were utilized for passenger and cargo transportation businesses. They recognize air safety is absolutely crucial to their businesses, and they do go to great extent to ensure that their members maintain and promote the highest standards of safety.

IATA Operational Safety Audit (IOSA) program is an example, as IATA now expects that all its members to have undergone this audit to standardize their safety readiness. IATA publishes annual reports on the safety performance of the global air transport industry that display Key Performance Indicators for the industry.

The International Air cargo Association (TIACA) is actively encouraging safety education and promotion amongst its members mindful that most cargo aircraft have had high usage and are of advanced age, and if not well maintained and operated, they could pose a threat to population centres near airports and those who live beneath their flight paths. Maintaining a holistic approach to business and air safety, TIACA positively encourages maintaining very high flight safety standards amongst its members, and moreover, generously support relevant research at universities through their scholarship schemes.

Given these noble ideals of international trade association, at grass root levels there ought to be the right balance between business needs and safety. Generally commercial and business policies of aircraft operators and maintenance providers tend to put pressure on funding available for safety improvements, pushing safety to a position of a "hygiene factor" as opposed to a "motivator" for investment. This is one of the areas that would come under scrutiny in this research study as a source that contributes to human error.

That said, IATA and TIACA were explicitly identified in the ID, but they had been considered together with other global issues that affected corporate policies towards CAW and safety.

A3.3.9 AAIB

The role of the Aircraft Accident Investigation Branch (AAIB) had been left out, because it was not an active participant to the CAW process. Its role would come into prominence only after a significant incident or an accident. However AAIB was mentioned in this document for completeness; some members of UK AAIB including its Chief Inspector have made advisory contributions to this research study.

A3.4 Factors common to groups

A3.4.1 Individual operatives

The role of the individual too needed to be considered in determining causal factors. Regardless of the quality and standards of training, an individual's inner make up, personal profile, age, memory retention, recollecting powers, capacity to handle climatic conditions, variations in light and sound, the way he reacted to domestic and work environment stresses, all such human factors needed to be considered.

Whereas there were training, qualification and licensing standards, there were no standards for the individual characteristics and how the individual should behave in response to external or internal conditions that were constantly in a state of transition. In that respect the only areas the industry and the law commonly recognized were the health and welfare aspects of employees, and the employer's duty of care to provide adequate support at the work place. However evidence suggested that the levels of support had still much to be desired, and in the current economic conditions those as well as personnel standards had been eroded away despite their qualification. That was an ideal basis for the generation of individual error at work place.

A3.4.2 Defences

It followed therefore that error contributions from any one of these peripheral groups ought to be resolved or eliminated before they caused more damage downstream, only if they could be detected in time. But errors that were undetected and lay dormant could eventually find their way into core group activities where they could manifest themselves and trigger incidents or accidents.

In mitigation of various hazards that existed in the CAW infrastructure and processes, defences had been set up by regulation or by the application of common sense. Regulation was legally binding and AO were expected comply with them. This ID represented these defences within both core group and peripheral groups, in the form of regulations applicable to the type of AO, e.g. Part 145 regulation.

But errors occurred when existing defences against potential hazards were over-ridden, when defence mechanisms were not set up due to lack of appreciation, foresight or prior knowledge of a consequence, or by simply creating conditions under

which CAW process could not be sustained as intended, e.g. withdrawing resources such as funding, manpower or time to do the work.

A3.5 Utility node

Thus, as already mentioned, given the existence of these sources of errors and shortfalls in the CAW process, either the delivery of a flight ready aircraft or the safety of the flight itself could be compromised. In such case, there could well be a degree of risk associated with the end product. The risk could be either actual or latent. The risk was actual if conditions associated with the error would lead to an incident; latent, if the error or its immediate consequences lay dormant as incipient failures, and then manifested themselves as actual failures at a later occasion when conditions got critical enough to trigger an accident.

Naturally, prior knowledge of this risk, both at critical and non-critical levels, had a value to business managers as well as to engineering operations managers. It was this "value" in monetary terms which was represented in the "utility node".

A3.6 Causal chains

Part of the analytical process was to establish the logic of causal chain between various CAW process activities within each participating groups as well as in between those groups. Nodes in the high-level ID, as it was, would not show this relationship openly. Therefore to obtain the necessary transparency, the high-level ID should be dissociated down to smaller elements of causal chains.

Intentionally Blank

Appendix 4

Relating CAW elements to BBN

A4.1 Introduction

States of Nature embedded in the nodes of a BBN identify if the relevant event is error free or has an error, and if it has an error, then to what causal factor it is attributed. For this purpose it is necessary to gain knowledge of hazards, root causes, available defences if any, and if the defence has failed.

A4.2 Hazards

Hazards are the dangers that exist in a system, which obstruct the achievement of the intended system's objective. Some hazards are more dangerous than others. Some hazards in a system may be blatantly obvious but they nevertheless get ignored by managers and operators of the system who may have other priorities, distractions related to business or if not due to their attitudes and values.

Other hazards are more subtle, remain elusive or lay dormant in the system, and then surface unexpectedly when combined with other similar latent hazards. Between these two extremes lay a whole range of dangers in between of different magnitude. Most of these hazards directly or indirectly lead to human error at the human-machine interface, which in turn could lead to incidents and accidents.

Analysis of hazards and identification of defences are the usual steps of any risk assessment exercise. However, this study is concerned with the quantification process of risk analysis, given hazards and defences within the process; the methods of minimizing the risk by either removing or mitigating the effects of hazards is outside the study remit. Therefore, the study has adopted a slightly different technique to deal with the analysis of hazards and defences.

Hazards in CAW are already well understood and much literature is available that provides hazard, error and defence taxonomy. Shappell and Weigmann (2003)[63] provide an excellent analysis of the human factors that lead to aircraft accidents. Reason and Hobbs (2003)[1] focuses more on the hazards that could occur in a maintenance environment.

A4.3 Defences

Much regulations and devices have been created to defend against hazards.

This study starts from the point that most hazards in CAW are already well understood, and that an adequate defences system is already in position to counter the hazards.

Therefore in this work, instead of reanalysing hazard, an assumption is made that, where there is a regulation there is a hazard. The regulation itself has been put in place as a defence, and therefore if the regulation is complied with honestly, then the risk attributed to the corresponding hazard would not arise.

This study has not repeated this operation, but it has made use of the data already available in the public domain. Causal factors identified in MEDA will be used.

A4.4 Strategic Level Hazards

Roots of some errors lay in higher level strategic policies and the way they are implemented. Examples are given in the following list. Often the hazard is created by the change of policy. This study is not criticizing the change but simply stating a fact that a change without adequate preparation to manage the change, as well as any resulting impact on resourcing, is a root cause.

A4.6 Global or Central Government Initiated

- New legislation on air traffic volumes, timings, pollution, noise, taxation
- Trade union laws.
- Open skies policies.
- Promoting competition.
- Reduction of oversight or accountability.
- More accountability without supporting evidence.
- Devolution of regulatory oversight
- Undermining regulator authority and capability.

A4.7 Corporate Business

- Reaction to central government policies requiring cut backs from operation.
- Market losses due to wrong financial decision
- Competition from business rivals.
- Response to Open skies policies and to competition
- Poor change management e.g. with introduction of new aircraft fleets or new technologies.
- Increasing passenger traffic without increasing own fleet
- Change of key personnel from board level downwards.

- Changes to organization infrastructure.
- Changes to Organizational Exposition for the approved organizations: routes, aircraft, airfields.
- Changes to support services.
- Change of location
- Changes to HR policies and pay and conditions.
- Changes to trade union relationships.
- Introduction of new business ventures
- Implementation of outsourcing policy.
- Weak or inadequately supported interface contracts.

Intentionally Blank

Appendix 5

Consequences

A5.1 UK CAA Classification of consequences

CAP 776 Global Fatal Accident Review 1997-2006[109] provides a listing of consequences that is used to record the either the accident type or the outcome of accidents. The top ten were:

- Post-crash fire
- Loss of control in flight following:
    - Technical failure
    - Non-technical failure
    - Icing
    - Unknown reasons
- Controlled flight into terrain
- Runway excursion
- Collision with terrain, water or an obstacle
- Forced landing on land or water
- Structural failure
- Emergency evacuation difficulties
- Fire, smoke, fumes during evacuation

In this study, that was limited to a controlled group accidents were a rare occurrence and it was necessary to device a more gentle scale of consequences, without disregarding the possibility that some errors could lead to catastrophic accidents. Some of these severe accidents would no doubt lead to monetary and other consequences, such as:

- Loss of prestige and /or loss of passenger confidence, manifested in loss of passenger numbers.
- Loss of business.
- Bankruptcy.

Since the study would be mostly uploading “bottom of the iceberg” type error. For them, consequences would be either “No Consequence” meaning the cost of correction was absorbed into routine cost of running the business, or into a larger cost of error that affected a scheduled flight. For completeness, consequences and conditionality were categorized as follows even if data were not available.

A5.2 Consequences considered for the study

A5.2.1 No consequence

- Error detected before task completed, corrected.
- Error detected during inspection, corrected.
- Error detected during documentation, corrected.
- Error detected during certification process, corrected.

A5.2.2 Potential or actual flight delay

- Error detected during pre-flight, corrected.
- Error detected during sign up for pre-flight, corrected.
- Error detected during walk-round, corrected.
- Error detected during ground handling, corrected.
- Error detected during aircrew cockpit checks, corrected.

A5.2.3 Actual flight delay, missed the slot time or flight cancelled

- Error detected during start up, corrected.
- Error detected during taxi or pre-take off checks, aircraft returns to dock and corrected.

A5.2.4 Return to dock

- Error detected during takeoff run, abort take off, risk to aircraft, crew and passengers.

A5.2.5 Flight returns to base or diversion

- Error not detected, take off, error detected, dump fuel and return to base.
- Error not detected, take off, and then manifests itself during the flight, diversion to other airport.

A5.2.6 Flight incident but carried risk of escalation

- Error not detected, takes off, manifests itself in flight, no incidence, no diversion, completes journey and correct.

- Error not detected; take off, error manifests itself as flight incidence, tolerable. Completes journey.

A5.2.7 Flight incident and controlled diversion

- Error not detected, take off, error manifests itself as flight incidence, tolerable but diverts to the nearest convenient airfield.

A5.2.8 Flight incident and emergency diversion

- Error not detected, take off, error manifests itself as flight incidence, intolerable and unacceptable. Emergency diversion to nearest airfield.

A5.2.9 Forced landing

- Error not detected, take off, error manifests itself as flight incidence, intolerable and unacceptable, and no time to lose, get the aircraft on ground/ water rapidly - crash land.

A5.2.10 Collision

- Error not detected, take off, error does not get detected nor manifests itself, and leads to collision with ground, fixed object or another aircraft.

A5.2.11 Structural failure in flight

- Error missed, aircraft departs, error leads to a structural failure in flight. Various cost consequences could result from this type of situations:
    - No casualties, damaged aircraft recovered to the nearest airport. No damage at ground level. Recovery costs.
    - No casualties in aircraft, damaged aircraft recovered to the nearest airport. Damage to assets on the ground and/ or ground causalities. Recovery costs.
    - Casualties in air and ground. Assets damaged. Aircraft recovered to nearest airport. Recovery cost.
    - Aircraft crash lands or breaks up in air. Total loss. Ground assets damaged and casualties.

A5.3 Monetary consequences of accident involving hull break up, fire, crew, passenger and 3rd party on ground

- Only aircrew and passenger causalities. And aircraft itself and hold contents
- Aircrew and passenger causalities, aircraft plus hold contents. Assets on the ground and ground causalities.
- Aircraft, Aircrew and passenger causalities, aircraft plus hold contents. Assets on the ground and ground causalities.
- Aircraft, Aircrew and passenger causalities and/or cargo Assets on the ground and ground causalities. Applicable to cargo aircraft.

A5.4 Other potential consequences.

- One or more aircraft of the fleet show incipient problems, affects aircraft availability, operation, short terms
- One or more aircraft of the fleet show incipient problems, affects aircraft availability, operation, long term.
- All aircraft of the fleet show incipient problems, affects aircraft availability, operation, short and long term. No effect on fleet replacement.
- All aircraft of the fleet show incipient problems, affects aircraft availability, operation, short and long term. Will affect fleet replacement plans.

It would not be an easy task to estimate the cost of such errors, on a case by case basis, even though this was the desired process. To categorize cost data from various possibilities, a cost scale from £10 to £1B (log to base 10) has been devised.

A5.5 Concept of a scale for cost of consequences

Monetary cost of consequence (£)	Log_{10} Scale = Consequence Scale	Remarks
1 -9	0	Negligible and may be ignored
10 - 99	1	
100 - 999	2	
1000 - 9999	3	Resolution may be increased in any practical application by progressively increasing the number of sub divisions in each medium level group. This would depend on the amount of data available. For upper end groups there will hardly be any data, thus making greater resolution impractical in those groups.
10,000 - 99999	4	
100,000`- 999,999	5	
1, 000,000 – 9, 999,999	6	
10, 000,000 – 99, 999, 999	7	
100, 000,000 – 999, 999,999	8	
1, 000, 000,000 – 9, 999, 999,999	9	

Table 5.5.1 – Cost Groups

Appendix 6

Sample data set – Airline A

Serial No	Description
A08/005	Aircraft released to fly, with a loose panel on a horizontal stabilator following Check servicing, Discovered one-month after releasing aircraft to fly.
A08/001	Door seal pressurization leading to accumulator explosion.
A07/027	Aircraft flew with undercarriage ground locks fitted. Forgotten to remove ground locks.
A07/026	Damage to port wing flap tab skin. Suspected contact with GSE.
	Attempted to drive a forklift truck beneath the wing of an aircraft.
A07/025	Engine chip detector inspection cleared on the tech log without first having completed the leak check. Two similar entries by different technicians on the same task.
A07/023	Un-commanded discharge of a fire extinguisher in cargo bay.
A07/022	Fuel spillage during aircraft refuelling in hangar.
A07/020	Pair of pliers found in between LH wing trailing edge and wing outboard flap. FOD hazard.
A07/019	GPU driven away while cable still attached to the aircraft.

- Ten reports were provided. One report was a duplicate copy of the other.
- One reported incident (A07/025) had been repeated on the same aircraft, on two different occasions and hence counted as two separate incidents.
- In A07/026 there were in fact 2 unconnected events of similar nature, i.e. mishandling of GSE in the vicinity of aircraft.
- The 10 reports generated 11 error incidents.

Intentionally Blank

Appendix 7

Analysis of sample data set from Airline A
Causal Factors and Causal Chains

7.1 Summary of Investigation Reports

Serial No	Event	Error	Causal Factors	Regulation/ Defence	Remarks	Management Challenge
A/08/005	Horizontal stabilator panel screws not fitted	Released to fly with a loose access panel	P - Failed inspection	Maintenance standard **Pt M -Sub part D** Maintenance procedures, standards and quality checks **Pt 145 - A65**	Miscommunication, access to the panel and poor visual perception directly contributed to the error. Access to job cards, and mechanics not always signing for their work were side issues, which though not relevant to this case were dormant errors in the system.	What is the Airline A's policy on resourcing, in this case sufficient access platforms? Is there a scale of equipment? How does organization deal with peak demands?
			C - Inadequate visual perception of surface			
			C - Mechanics failing to sign for work done.			
			C– Mechanics had no access to job cards			
			C - Miscommunication	HF		
A/08/001	Door seal pressurization reservoir explosion	Unauthorized procedure	P - Lack of right equipment	**Part M-Sub part D** regarding failure to comply with given AMM instructions **Part 145-A40** re tools and test equipment unavailability and failure to identify alternative tools	Absence of Oracle data at the right place and consequent use of unauthorized practice (based on local culture) were the primary causes. Though not covered by the report, it seems that QA had missed this shortcoming. A routine review of scale of equipment for tasks would have been beneficial. Lack of a Pressure Relief Valve in the design is of concern.	- Does the company review scales of equipment and inventory? - Is this part of QA checks? - Has the design shortfall followed up?
			C - Inventory failed to identify AMM equipment and fails identify alternative equipment available			
			C- Carry forward company wrong practices, and failure to rectify repetitive mistakes. QA issue.	QA missed or poor reporting or both. **Part 145-A65** standards and Quality checks		

Notes:
Causal factors
P = Primary
C= Contributory

Serial No	Event	Error	Causal Factors	Regulation/ Defence	Remarks	Management Challenge
A 07/027	Ac took off with UC ground lock fitted	Omission (of technical procedure)	P - Failure to record in the operator's technical log, the disabling of the undercarriage by fitting of ground lock and calling for its removal and post-ground run PDI	Recording of maintenance tasks **Pt 145 A50**	Forgetting to remove the lock was the primary error, whereas by not raising a log entry, a defence was breached. Time pressure, local manning level, and multi-tasking were the main contributory factors. Review of the timing of PDI had already been undertaken.	What is the Airline A policy on documentation on running repairs? Because of urgency to get the flight underway, are procedures for handling running repairs different from the norm?
			C- Time pressure	HF		
			C- Resource shortfall in Line maintenance, engineer undertaking other parallel control/ communication tasks	Adequate manning **Pt 145 A30**		
			C- Regulations that seemed to have eliminated engineer pre-dispatch inspection (PDI), followed by final aircrew walk round.			
			C- Timing of PDI relative to rectification work.			
A 07/026_1	Damage to port wing flap tab skin	Violation of rules	P - Non-segregated facility	Inappropriate facilities **Pt 145 A25**	Conflicting usage of space was the primary cause, and space appears a critical issue.	What is Airline A policy on resourcing for facilities when space becomes critical?
			C - No free access path to GSE			

Serial No	Event	Error	Causal Factors	Regulation/ Defence	Remarks	Management Challenge
A 07/026_1 (Error 2)	Attempt to drive forklift beneath the wing	Violation of rules	P - No segregated facilities	Inappropriate facilities **Pt 145 A25**	Near miss damage of an aircraft by forklift due to conflict in space usage is the principal causal factor. Contributory human factors should be assessed against the fitness of the individual to work in an aircraft environment, as he appeared to be sensitive and already functioning under long term stresses. Such people tend to be highly susceptible to making errors.	What is the Airline A HR policy regarding employment of personnel, needing health and welfare attention, in an aircraft environment?
			C - No free access path to	Inappropriate facilities **Pt 145 A25**		
			C - Health and welfare issues/	Individual **HF**		
			C - Multitasking	Individual **HF**		
			C - Communication shortfalls at task handover	Group **HF**		
			C - Lack of documented procedures	**Pt 145 A45**		
			C - Noise, Distractions and interruptions	Group **HF**		
			C- No shift handover, Production planning	**Pt 145 A47**		
A/07/025_1	Magnetic chip detector inspection. Task certified completed before its completion	Procedure not followed	NK	**Pt 145 A50**	This earlier error in the certification triggered off the incident reported in A07.025. Both errors considered as 2 similar back to back errors	Is this an indication of an unauthorized practice to economize on time and energy? HR policy forcing this situation on engineers?
			No shift handover, Production planning	**Pt 145 A47**		

Serial No	Event	Error	Causal Factors	Regulation/ Defence	Remarks	Management Challenge
A/07/025_2	Magnetic chip detector inspection, certified completed before completion	Procedure not followed **Pt 145 A50**	P- Time pressure or convenience or both acting together (insufficient information to discriminate if time pressure is actual or perceived)	Production Planning, **Pt 145 A47** Group **HF**	This is mainly a manning issue, but suggests the existence of local unauthorized procedures to economize on time and energy by way of compensating for the time pressures.	What is Airline A's manning policy, especially when dealing with geographically separated work sites and peak demands? What is the actual performance against expectation in response to authorized manning levels?
			C- Inadequate manpower - short term	Manning **Pt 145 A30**		
			C- Workplace interruptions	Group **HF**		
			C- Multi-tasking	Group **HF** Production planning **Pt 145 A47**		
			C- Miscommunication between engineer and aircrew	Group **HF**		
A/07/025 Other errors noted during investigation issues		Incorrect authorization of personnel		**Pt 145 A35**	This is a dormant error	Why QA checks missed this? Policy on non LAE in QA role?
A/07/025 Other errors noted during investigation issues		Incorrect technical reference/maintenance data		**Pt 145 A45**	This is a dormant error	Why QA checks missed this? Policy on non LAE in QA role? Non LAE QA depending on LAE's whom he audits for specialist advice?

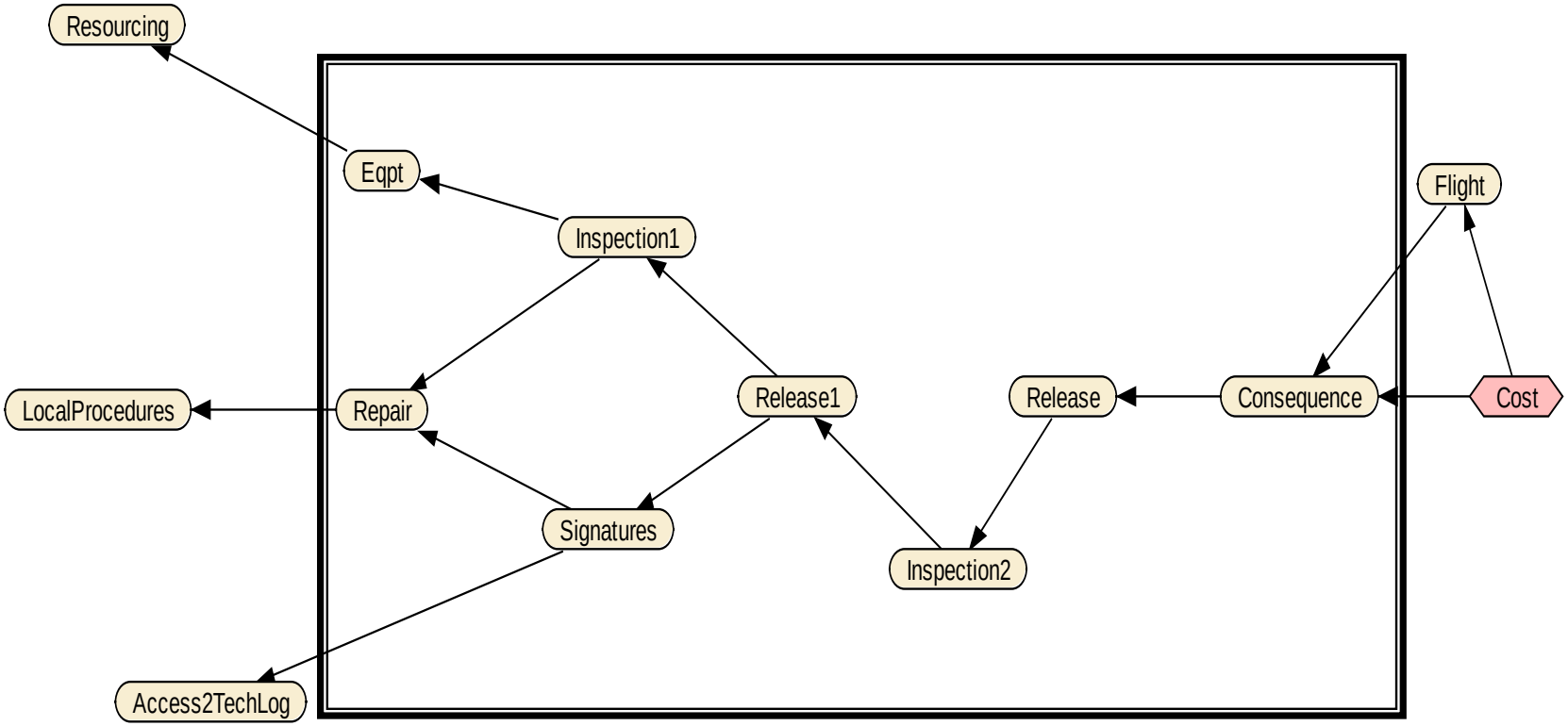
Serial No	Event	Error	Causal Factors	Regulation/ Defence	Remarks	Management Challenge
A/07/025 Other errors noted during investigation issues		Amendment state of Form ADA 1001		**Pt 145 A45**	This is a dormant error	Why QA checks missed this? Policy on non LAE in QA role?
A/07/023	Uncommanded discharge of cargo bay fire extinguisher	Procedure not followed	P- Overridden procedures on account of inadequate trade knowledge on type	Competency **Pt 145 A30**	Knowledge shortfalls and overconfidence led the engineer to make this error. Supervision could have avoided the incident. But supervision dependent on local manning level.	What is the Airline A policy on employing less experienced personnel without supervision? How does Airline A compensate for shortfalls in system knowledge?
			C- Unfamiliarity with this cargo bay FE system fitted to American operated aircraft.	TNA shortfall Competency **Pt 145 A30**		
			C- Inadequate system knowledge	Competency **Pt 145 A30**		
A/07/022	Inability to contain fuel spillage in hangar	Inadequate equipment and materiel resources	Inadequate planning (for larger spillages)		Planning limitation and poor husbandry re empty kit in hangar H21	Standby fire tender during hangar refueling may be more relevant? Is there a design shortfall?I

Serial No	Event	Error	Causal Factors	Regulation/ Defence	Remarks	Management Challenge
A/07/020	Loose pliers found wedged between the LH wing trailing edge and leading edge of LH wing outboard flap	Loose article in aircraft control system	P-: Failure to complete tool check	Maintenance standards **Pt M Sub Part D 402**	This case seems to be an over-reaction to cover up for a simple case of failing to check and account for all the tools taken to an aircraft, given that the engineers were competent enough to overcome all other handicaps placed on them. May be the Airline A tool control policy is such that an engineer does not know how many tools he takes to the aircraft and how many he takes away from the aircraft	What is the Airline A policy on tool control?
			C- Local instructions missing	Maintenance procedures **Pt 145 A65**		
			C- Task not properly assessed	Maintenance procedures **Pt 145 A65**		
			C-: Deviations from procedures	Maintenance standards **Pt M Sub Part D 402**		
			C-: Environmental conditions and poor lighting.	**Pt 145 A25**		
			C-: Unavailability of equipment and specialist tools caused interruption	**Pt 145 A40**		
A/07/019	GPU driven away while it was still connected to the aircraft	Damaged equipment	P- Complacency	Individual **HF**	This appears to be a simple case of complacency. Evidence does not substantiate fatigue or insufficient experience.	Support workers, do they have written procedures? Is 6-month working not enough experience? Why was the worker fatigued out 2-hrs into his shift. Was he doing a second job when off duty? Airline A HR policy?
			IC- insufficient experience, lack of training or competency.	Competency **Pt 145 A30**		
			C- Fatigue.	Individual **HF**		

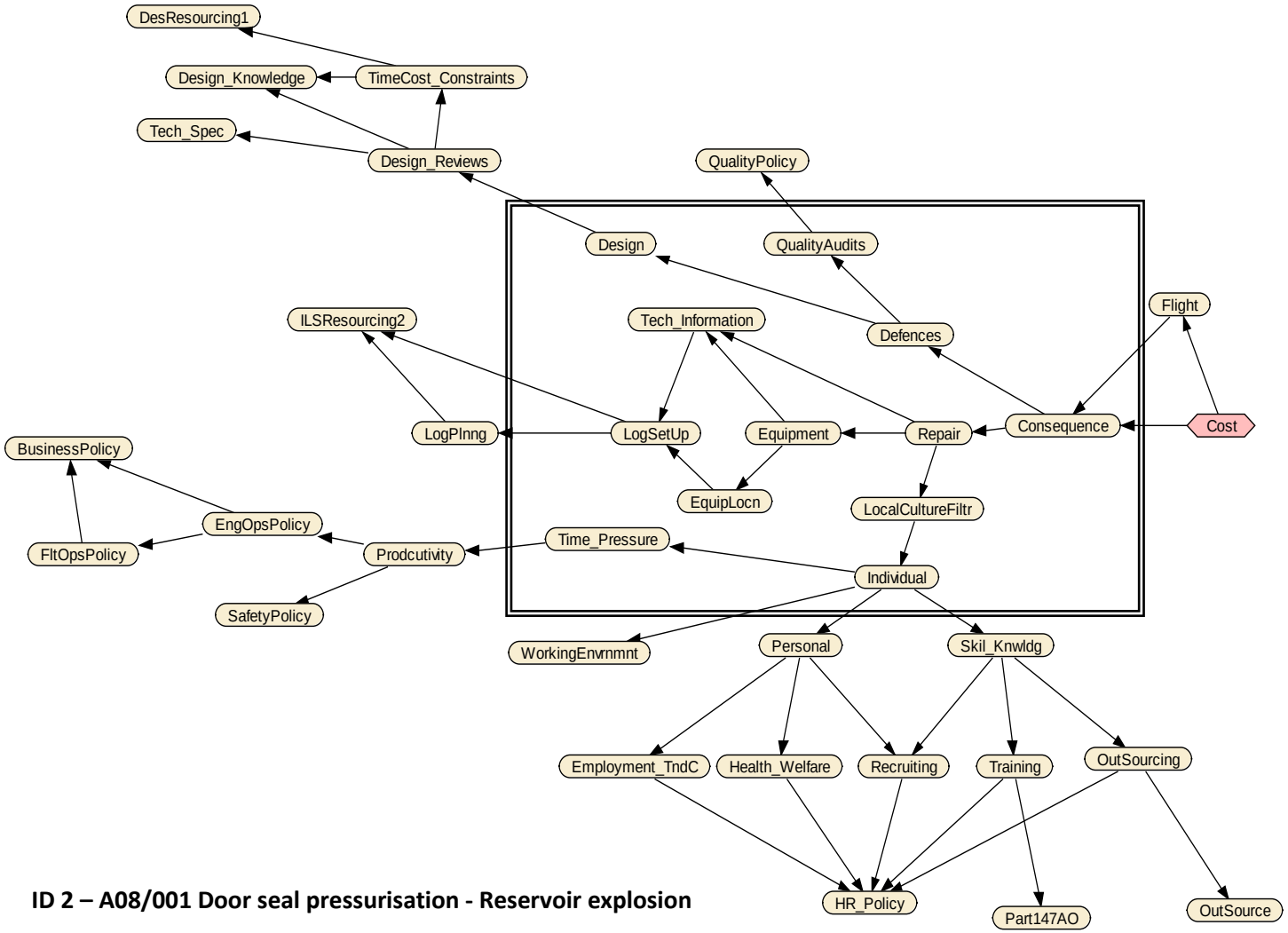
7.2 Tracing causal chains in a system fault

A causal chain is explained here with an example. An incident primarily due to a shortfall in a "work card" could be progressively traced to an error in Part 21 organization that designed, produced the AMM, as well as to the work card drawn up on the basis of the AMM, to shortfalls in supervisory and review functions of superiors. It could also be due to shortfalls in quality audits system: for example, the quality audit program might have not accommodated this area relating to the review of AMM and work cards. If the AMM review requirement is already in the quality plan, then it might be possible that the plan has not been implemented, or alternatively if it was in the plan, then implementation had been unsatisfactory. Relevant Part M and Part 145 regulation might have been breached too, and it might be relevant to examine if this area had been audited by the Regulator during oversight inspections and what the outcome was.

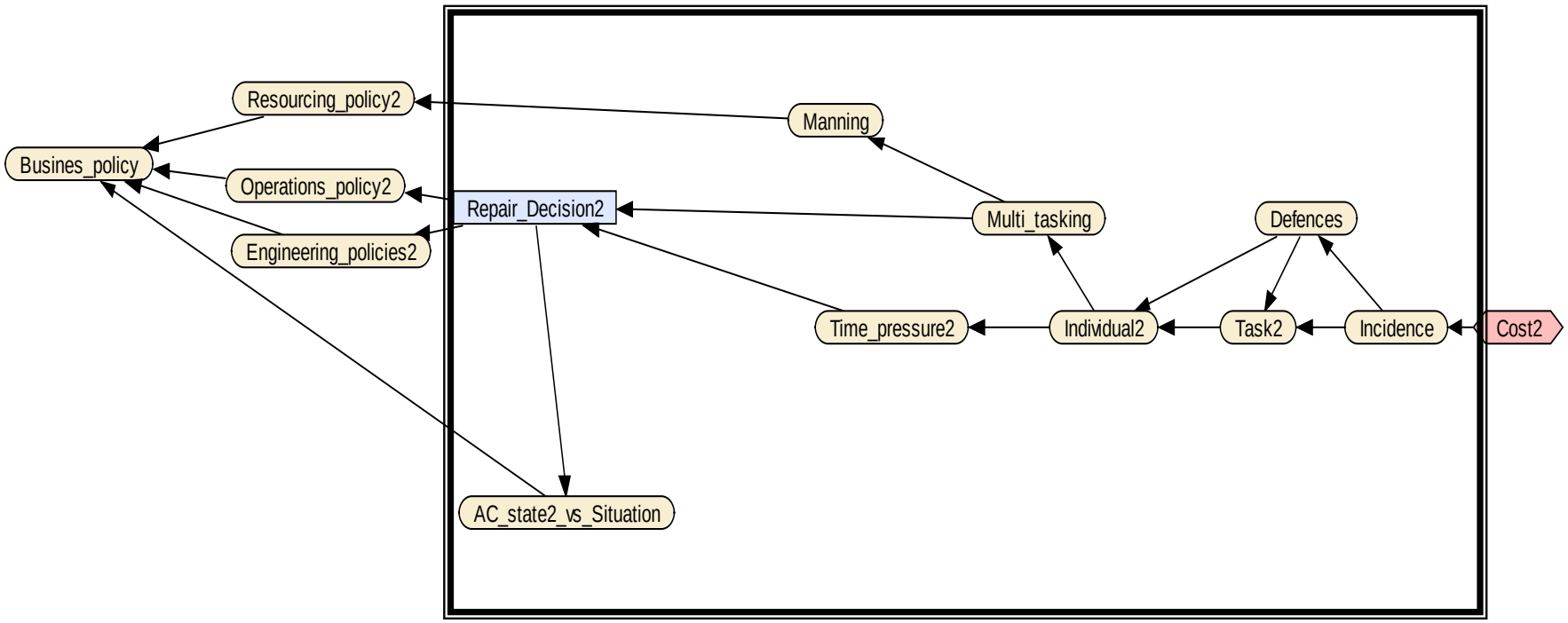
Causalities of the following incidents have been traced back starting from the incident. Causal chains within the framed areas had been undertaken by the operator's internal investigation. The study found that causal chains could be further extended, beyond what is fondly called in the profession as "management glass-walls". Often, such limitations of internal investigations are attributed to low cost-effectiveness as a way of generalization. But in reality it may be due part to the absence of contract cover, fund limitations, local sensitivities or management decisions to contain the error and its consequences within their span of control. The causal chain extensions in the following case studies have been reviewed by the data provider, and agreed as rational, with the reservation that their agreement is only for the purposes of academic research undertaken by this study program.



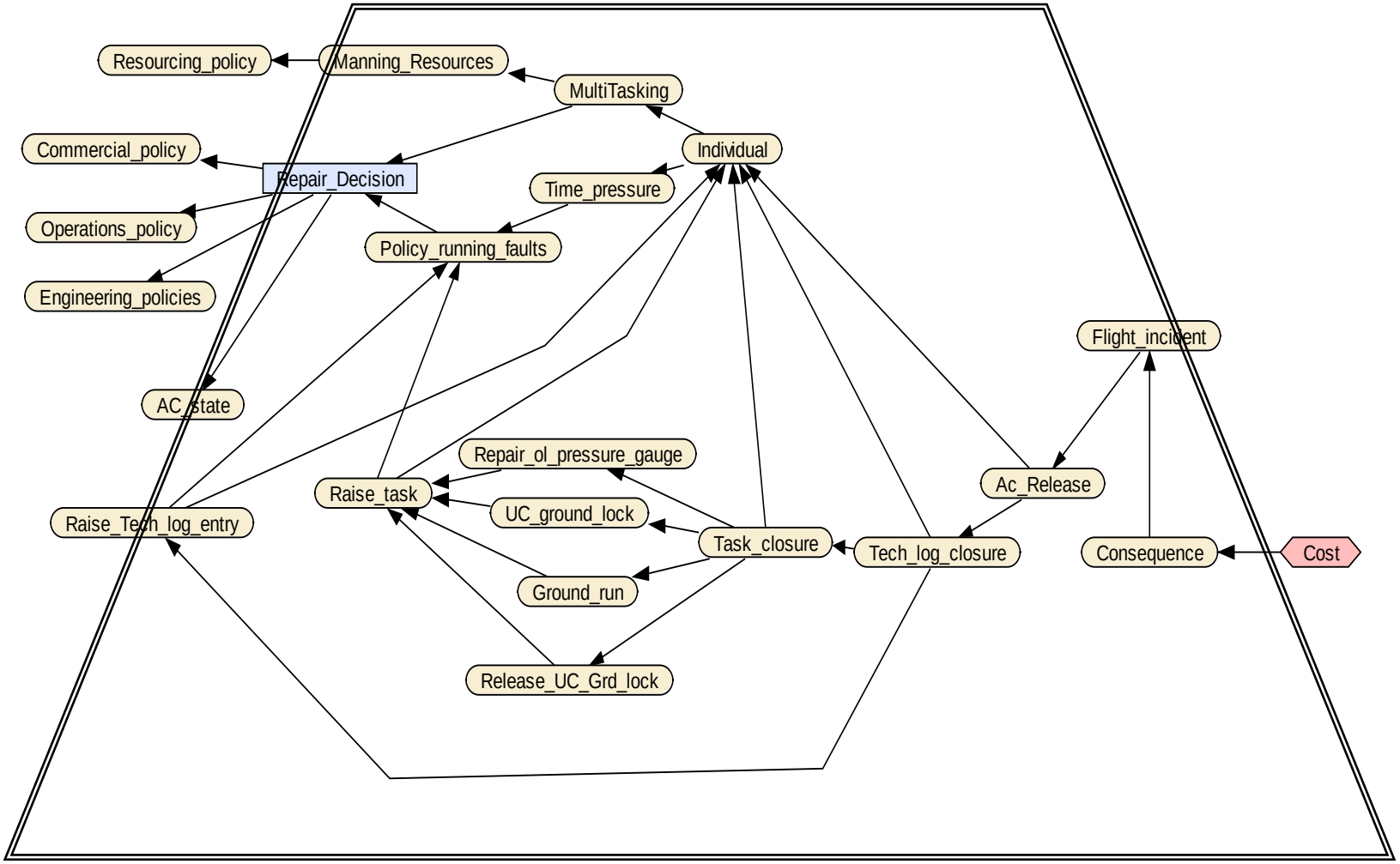
ID 1 – Loose screws on tail plane A08/005



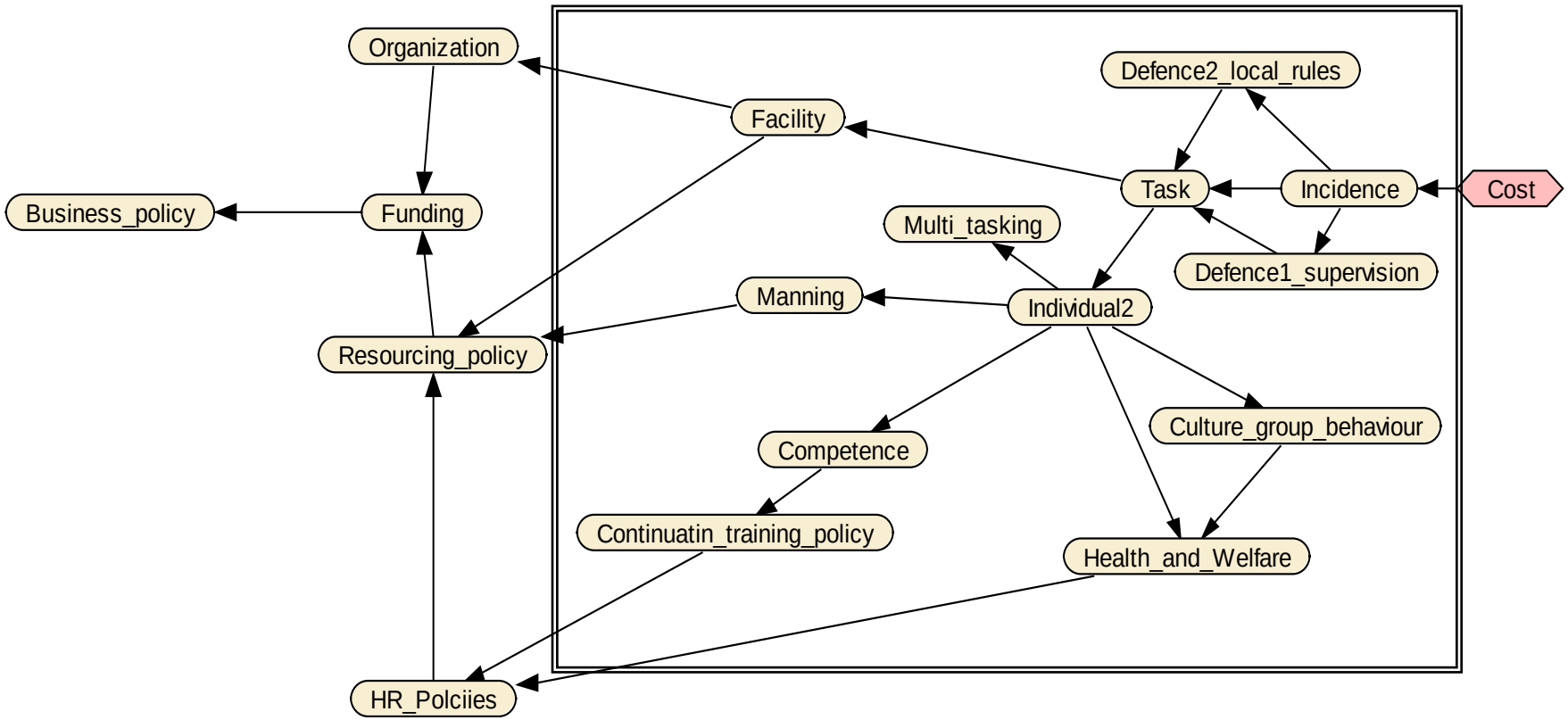
ID 2 – A08/001 Door seal pressurisation - Reservoir explosion



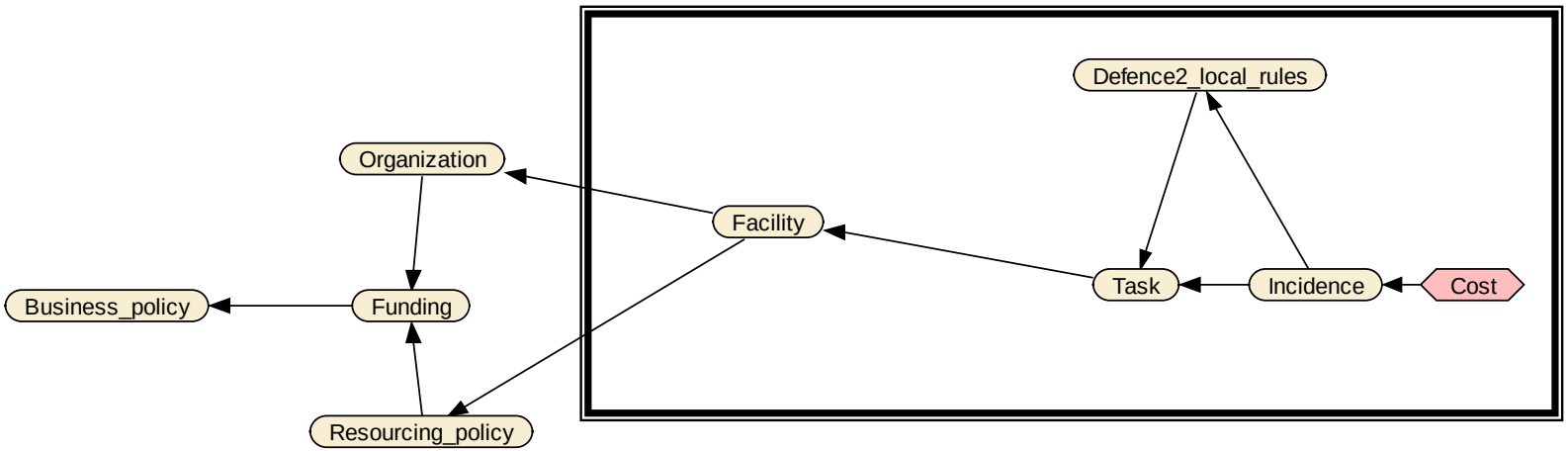
ID3 – A07/027 Aircraft flew with UC locks fitted_2



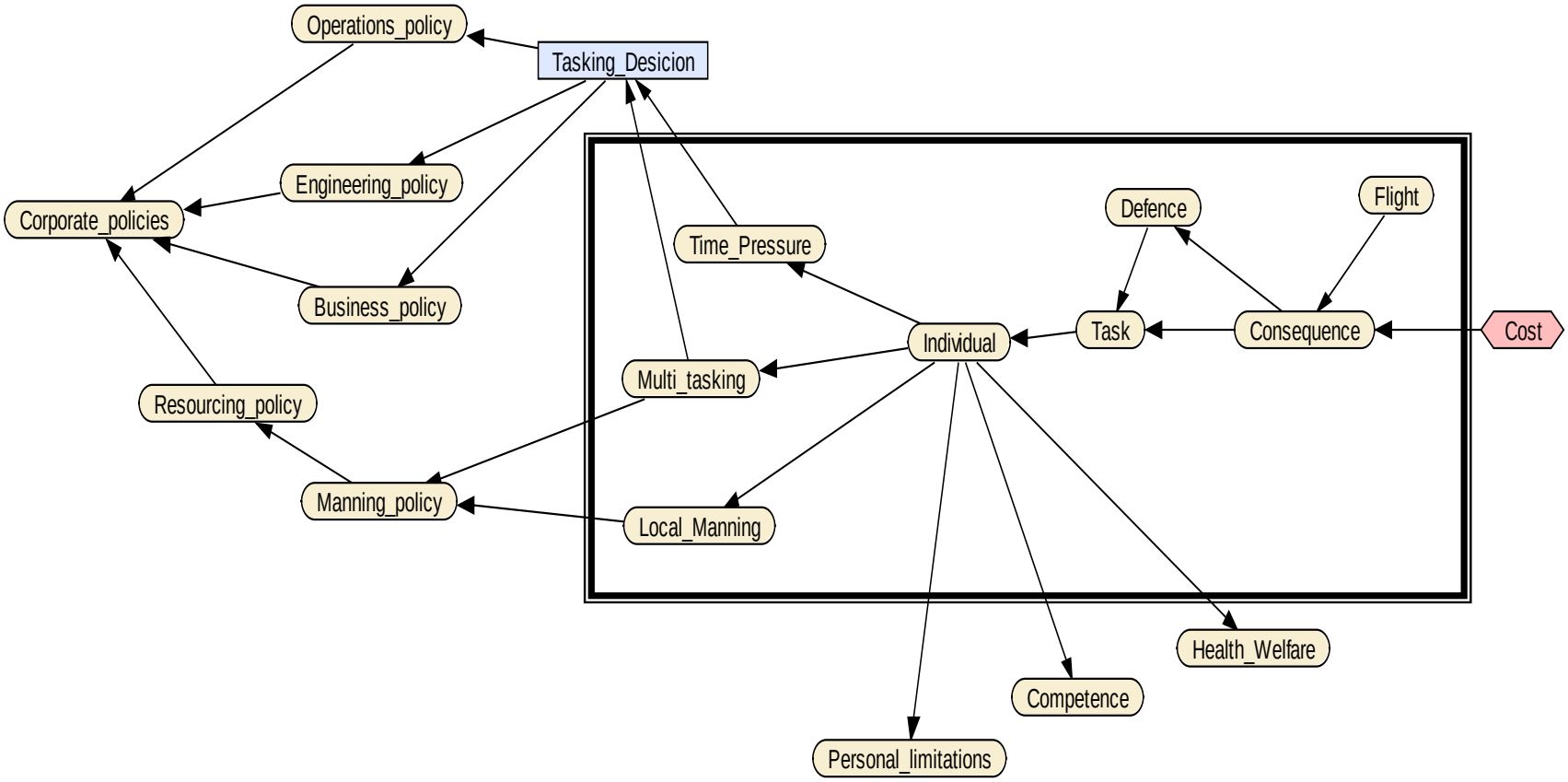
ID3 – A07/027 Aircraft flew with UC ground locks fitted



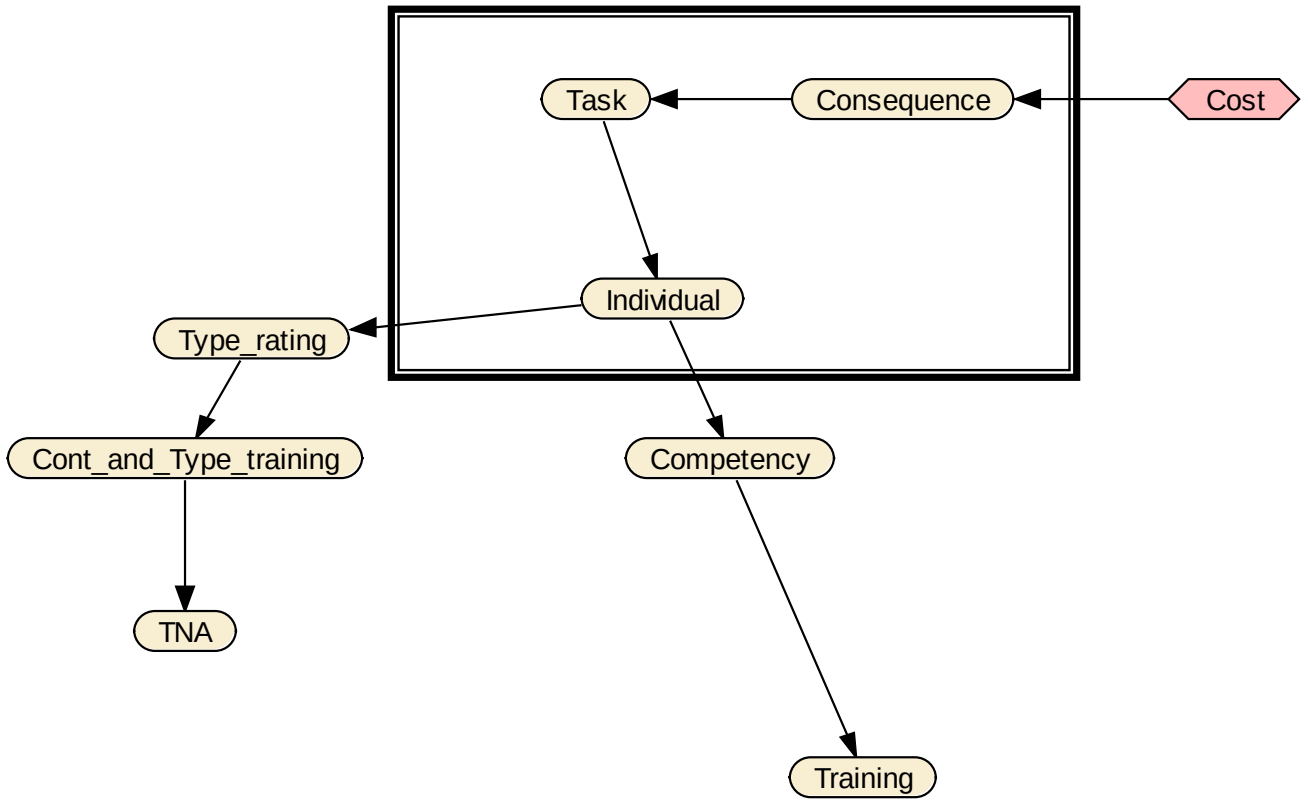
ID4 – A07/026 Damage to port wing flap tab skin



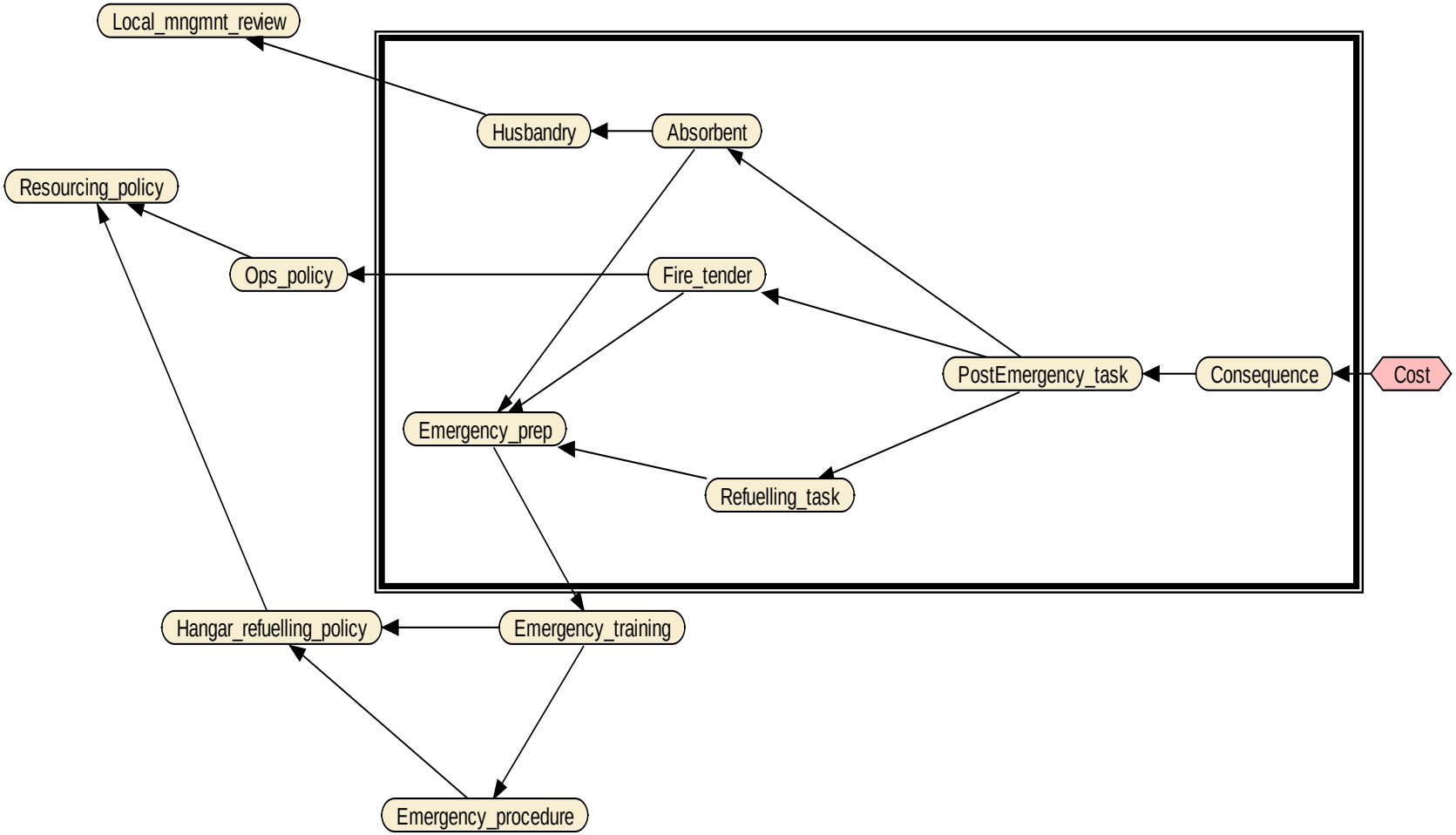
ID5 – A07/026 Damage to port wing flap tab skin_2



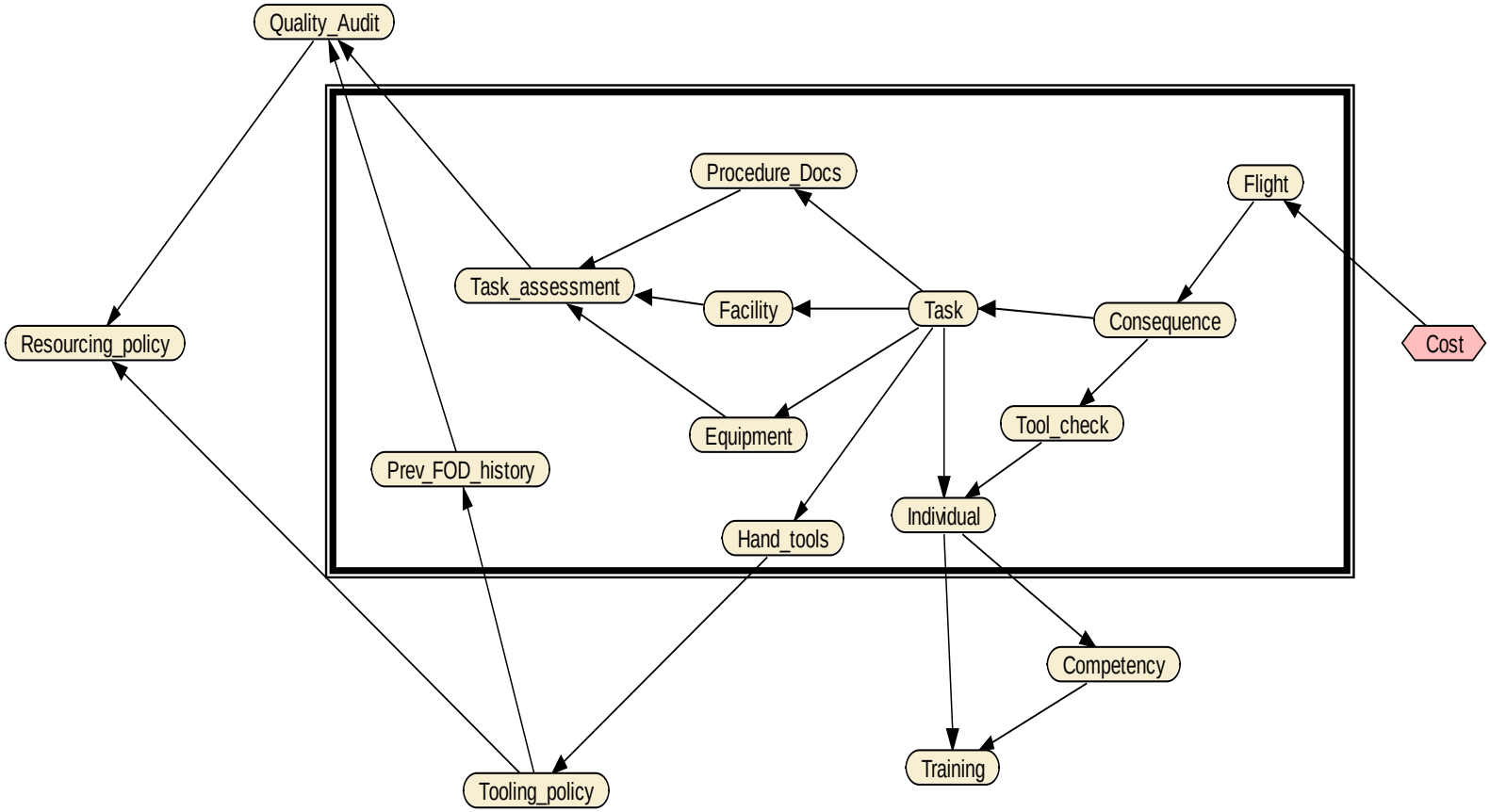
ID6 – A07/025 Incomplete magnetic chip-detector task



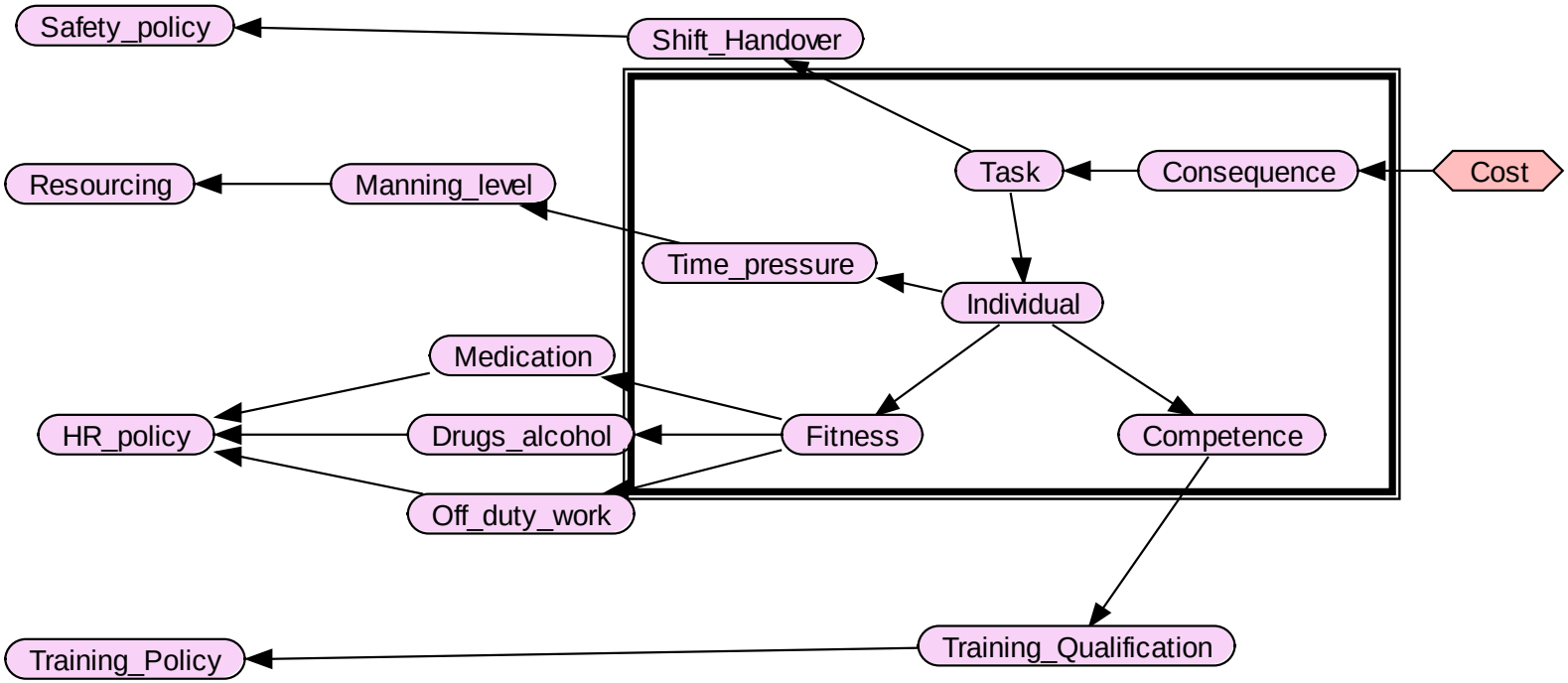
ID7 – EP07/023 Un-commanded discharge of fire extinguisher



ID 8 – A07/022 Fuel spillage during hangar refuelling



ID 9 – A07/020 Pliers found in wing/flap interface



ID 10 – GPU towed & power cable damaged A07/019

Intentionally Blank

Appendix 8

Comparison of three different management approaches to risk containment

Intentionally Blank

Comparison of 3 different management approaches to risk containment – Influencing factors on risk

Management approach	Compliance with regulation	Size of operation Vs capability	Operational performance	Safety & quality defences	Change management	Culture and Organizational set up	Risk contained?
RAF Structural integrity policy	Policy on fatigue life of critical components Statement of Operating Intent Y-coded items Structural Integrity inspections Fatigue meter fitted or digital operational loads measurement Policy compliance	Fleet sizes and marks Age Roles Data collection methods, storage, analysis , dissemination infrastructure: equipment, ground stations facilities, personnel, training (quantities and spread) Size of work load from regulator (staff officers) viewpoint, but also same related to aircraft in one RAF station relative to local commanders assessment of workload	Implementing fatigue monitoring Collecting data Analysis and dissemination Key performance indicators Trends etc	Fatigue test Dedicated Structural Integrity Working Groups for each aircraft type manages all structural policy and strategy Review of compliances results Analysis of fatigue outputs and SOI reviews Education New OLM programmes	Central change management by SI WG. Review of Statement of Intent for parametric changes New formations Defence policy changes New equipment Material changes SI or Fatigue policy changes Review of field experience	One owner. Highly accountable. Doctrinaire. Highly regulated by policies and rules of procedure. HR and Personnel management policy. Recruitment based on aptitude. High quality training. Personnel proactive. Organizational interfaces well controlled.	Yes most of the time. Still failures occur due to: Unreported usage. Deviation of product from design. Corrosion. Pilot error, operating outside limits. Historical data missed. Limit of knowledge

CAA-NL Risk model to implement RBO concept	Compliance with regulation , integrated with quality under Quality Risk: detail	Size and scope of work from regulators work load viewpoint. Number of approved organization. Numbers employed. Number aircraft. Number of standard inspection required by ICAO guideline, 2-yr cycle. Balance of production volume. Complexity of processes and equipment.	Variable due to different operators. Individual performance assessed from evidence during oversights	Quality risk: detail combined with column 2	NK	Safety culture HR policies Worker/management attitudes to safety, incidents and errors Communication and relationships Organizational behaviour Complexity Geographical spread Policies on outsourcing and subcontracting Productivity and innovation Attempts to measure	Yes but incidents occur. Unreported usage. Deviation of product from design. Pilot error, operating outside limits. Historical data missed. Limit of knowledge.
UK CAA ROWI Model Managing task loading for inspectors	Compliance with regulation Safety issues: Num Level 1 and Level 2 findings for previous year	**AOC Holder:** No of aircraft. A1, A2, A3 aircraft (our interest A1 ac only >5700kg. Number of QA staff. Tech planning staff. Nature of approved maintenance programme (intensity). ETOPs/ RVSM/ AWOPS, MNPS approved. **Safety issues:** Numbers and types of ac, FW or helicopter. Number in each fleet.	Variable due to different operators. Individual performance assessed from evidence during oversights	Number QA staff (but in capability, this column deals with defence performance) for both AOC Part M, Part 145 AO	Under safety issues: Num of operation's resources variations issued over previous year	Independent operators. Guard their independence and culture. Commercial competition. Safety culture observed but not measurable.	Yes but incidents occur. Unreported usage. Deviation of product from design. Pilot error, operating outside limits. Historical data missed. Limit of knowledge.

		Num MOR submitted Average age of aircraft Average hours flown per month **Part 145/Part M Org:** Number of A1 ac > 5700kg. Line types approved. A1 base types approved. Number of B ratings approved. Number C ratings approved. Number specialized services (like NDT). Number certifying staff employed. Number AOC supported. Num QA staffs. **Safety Issues:** For C rating companies only, the number of Form 1 issued previous year. Number of aircraft maintained. Number of Part 145 related MOR submitted previous year. Number of Level 1 findings previous yr. Num of Level 2 findings previous yr. Average age of aircraft maintained. Num maintenance resource .variations issued over previous yr.					

Intentionally Blank

Appendix 9

Data requirement issued to operators

A9.1 Way Forward

This note describes data requirements for the CAW Risk Model Research Study Program, as envisaged at present. As experience is gained it might be necessary to gather additional information; these will be discussed with data providers as and when required.

A9.2 Data Requirement

Subject to discussion and further refinement, three groups of data are requested.

- The first group of data will be used to define the boundaries of the reference frame of the controlled group.
- The second group will be the main bulk of data. It should consist of incidence and investigation reports in hard copy form or if not as digitised data files. If these reports have been already analysed into causal factors and categorised into digitised data files, then they may be of interest to the study, subject to their transportability and readability.
- The final data group will be supporting data, to be used for analyzing and interpreting main causal factor data. There is also a need to collect data on flights not affected by CAW errors.

A9.3 Boundaries of the controlled group

Define experimental period: Start date and terminal date. To maximise data capture, start date could be from the time airlines database reached a steady state since its formation. Terminal date is left open for the time being; it will depend on the size of data set available.

A9.4 Error and report types of interest

For the defined period, Airline A is requested to provide all investigation reports related to human error in CAW, regardless of the source, e.g. MEMS, AOR, and GOR etc.

Errors might have occurred at man/machine interface, or traceable back to organizational level, to task definition, integrated logistic support planning or implementation, approved organization/ regulator interface, or within Part 21 organization.

Regarding errors in Part 21 organizations, the study program is interested in error incidences and associated data related to post development services, modifications, or integrated logistic support. Errors occurred prior to the initial type certification would not be searched in this error trawl. However, if CAW process revealed prior errors, then these errors would be taken into account in this research as contributory factors that affected CAW process.

Internal investigation and closure reports on incidences that had been the subject of an MOR would be of special interest to this study.

Statistics on internal reports of unsatisfactory features in technical documentation, tools and test equipment, spares etc will be useful.

All internally reported incidents that involve the aircraft, passengers, crew or third party should be included.

A9.5 Background data of the incidents

For authenticity and validation of research work, it is necessary to identify where error data is coming from. Therefore, following information is required for each error report.

- Date
- Flight Number
- Aircraft Registration number
- When and where occurred or discovered, e.g. type of maintenance or audit check, oversight etc.
- Accumulated hours flown/ landings and take off/ sectors flown at the time of incidence or error.

Data source, Aircraft ID, Flight Number, Aircraft Registration Number, Location, Names of any individuals involved, and such raw data that is considered as sensitive information will be removed from any public-domain document that will be published at the end of the study program. Any data intended to be published would be desensitized. Raw data will be securely stored, and will be inaccessible to the public, until the end of a prescribed period when they will be destroyed.

A9.6 Supporting Data

- Corresponding to the time frame, error data should be related to
    - Utilization of aircraft in flying hours by type of aircraft.

- Alternative utilizations indicators: Number of sectors (or flights) flown, landings and take offs by type.
- Number of passengers flown.
- Number of aircraft in the register (owned as well as leased by the company for passenger flying)
- Number of aircraft actually flown in the month (month by month)
- Number of aircraft in Base servicing in the month.
- Base or check servicing programme, floor loading data.
- Number of flight crews per aircraft (by type).
- Rate of generation of base servicing or check servicing, e.g. servicing arising frequencies.
- Work force strength and profile by each organization: professional level, numbers. Month by month
- Number of flights dispatched, arrival at destination, diversions.
- Number of flight incidents and accidents related to CAW error, data to be linked to reported error.

A9.7 Statistics on "No Incident" "No Error" Flights and Sectors

Just as much as the study is interested in incidences attributed to errors, it is also interested in flights or sectors flown, and flying hours flown when there had been no incidences.

This information is necessary in order to represent the true state of nature of the organization, otherwise error data only would make the organization appear more hazardous, and of course at a higher risk when it should not be.

Intentionally Blank

Appendix 10

Nodes and States of Nature – Names and their disposition in the network

This Appendix lists the names of nodes used in the CAW Risk Model. Names of the states of nature could be read off from the Taxonomy details in Appendix 12.

This Appendix has been presented as a Look up Table to trace the distribution of nodes and states of nature within the model.

Certain nodes (indicated in italic) are critical nodes that combine the effects of error probabilities of upstream nodes. In this model they are referred to as accumulators. In the CAW process, the role of some of these nodes is equivalent to the line manager of a section (of engineers) checking and certifying that the output from the group is satisfactory.

There is an implicit defence activity embedded into each node, accumulators and others, but not shown. For example in the case of a proactively detected error at any node, it is assumed that the detection would lead to a defence so that the error would not be carried forward as an error if properly defended. Similarly an error previously generated in an upstream node, but missed there, could get detected at an accumulator node downstream. However, if an upstream generated error was missed at the accumulator, then the error would be registered at the accumulator too, whereas a defended error would not be.

Table A10.1 – Nodes and States of Nature

ID	Node	Num of States of Nature	Cum Total	Num of Nodes	Cum Tot - Nodes & Accumulators
	High Level Factors				
1	Global Factors	13			
2	Central Government	7			
3	Local Government	5			
4	Corporate Board	11			
5	Trade Union	9	45	5	
	Corporate Policy				
6	CEO AM Decisions	8			
7	Commercial Policies	6			
8	Flight Operations Policies	2			
9	Engineering Operations Policies	7			
10	Logistic Support Policies	8			
11	HR Policies	9			
12	*Corporate and Policy Issues*	*2*	87	7	12/1
	Change Management System				
13	Business Management	5			
14	Operations	7			
15	MOE	6			
16	Engineering and Technology	9			
17	Human Resources	8			
18	*Change Management*	*2*	124	6	18/2
	Size and Type of Operation				
19	Aircraft Type Series FW	13			
20	Aircraft Type Series RW	13			
21	Registration No	13-100			
22	AC Age	11			
23	Sectors Flown	11			
24	Full Maintenance Cycles	11			
25	*Aircraft*	*2*			
26	Ac Generation Time	4			
27	Operational Role	9			
28	Route	5			
29	*Nature of Operation*	*2*			
30	Flight Origin	14			
31	Destination	14			
32	Departure Time	13			

33	*Geographic Location Time*	*2*	261	15	33/5
	Technical Resources Capability				
34	Fleet Size to TR Cat A Staff	4			
35	Fleet Size to TR Cat B1 Staff	4			
36	Fleet Size to TR Cat B2 Staff	4			
37	Fleet Size to TR Cat C Staff	4			
38	Fleet Size to Non Cat Tech Staff	4			
39	*Tech Staff*	*2*			
40	Fleet Size to Logs Staff	4			
41	Fleet Size to Tech Managers	4			
42	*Other Support Staff*	*2*			
43	*Staff Complement*	*2*			
44	*Operation Vs Capability*	*2*	297	11	44/9
	Pt M and Part 145 AO Compliance				
45	Part 145 AO Findings L1	18			
46	Part 145 AO Findings L2	18			
47	*Compliance 145*	*2*			
48	Pt M Sub Part B Findings L1	3			
49	Pt M Sub Part B Findings L2	3			
50	*Part M Sub Part B Compliance*	*2*			
51	Pt M Sub Part C Findings L1	8			
52	Pt M Sub Part C Findings L2	8			
53	*Part M Sub Part C Compliance*	*2*			
54	Pt M Sub Part D Findings L1	4			
55	Pt M Sub Part D Findings L2	4			
56	*Part M Sub Part D Compliance*	*2*			
57	Pt M Sub Part E Findings L1	5			
58	Pt M Sub Part E Findings L2	5			
59	*Part M Sub Part E Compliance*	*2*			
60	Pt M Sub Part G Findings L1	14			
61	Pt M Sub Part G Findings L2	14			
62	*Part M Sub Part G Compliance*	*2*			
63	Pt M Sub Part H Findings L1	3			
64	Pt M Sub Part H Findings L2	3			
65	*Part M Sub Part H Compliance*	*2*			
66	Pt M Sub Part I Findings L1	6			
67	Pt M Sub Part I Findings L2	6			
68	*Part M Sub Part I Compliance*	*2*			
69	*Compliance M*	*2*			
70	*Part145 Part M Compliance*	*2*	439	26	70/19

	Quality Management System				
71	CAW Quality Policy	3			
72	Quality Plan and Program	6			
73	QA Scope	15			
74	Resources and Training Standards	9			
75	Audit Procedure	9			
76	Remedial Action Procedure	6			
77	CAW Management Activity	11			
78	Monitor Effectiveness of AMP	3			
79	Maintenance Contract Monitoring	11			
60	*QMS Policy Plans Scope*	*2*			
81	*QMS Tasks Processes*	*2*			
82	*QMS Organization*	*2*			
83	Pt M Management Activity	12			
84	Pt M Finding Reporting	4			
85	Pt M Corrective Action	4			
86	*Part M QA Performance*	*2*			
87	Pt145 Activity Area	15			
88	Pt145 Finding Reporting	4			
89	Pt145 Corrective Action	4			
90	*Part 145 QA Performance*	*2*			
91	Sub Contractor Activity Area	2			
92	SC Finding Reporting	4			
93	SC Corrective Action	4			
94	*Sub Contractor QA Performance*	*2*			
95	Supplier Activity Area	2			
96	Supplier Finding Reporting	4			
97	Supplier Corrective Action	4			
98	*Supplier QA Performance*	*2*			
99	*QA Performance*	*2*			
100	*Quality Management System*	*2*	593	30	100/28
	Pt M Pt 145 (and Pt 21) Combined Performance				
	Part 21 Organization				
101	Pt 21 Sub Part A General Provisions	5			
102	Pt 21 Sub Part B Type Certificates	22			
103	Pt 21 Sub Part D Changes To TC	10			
104	Pt 21 Sub Part E Supplemental TC	12			
105	Pt 21 Sub Part F Production without POA	11			
106	Pt 21 Sub Part G POA	17			
107	Pt 21 Sub Pt H Airworthiness Certificate	11			
108	Pt 21 Sub Part I Noise Certificates	8			

109	Pt 21 Sub Part J DOA	16			
110	Pt 21 Sub Pt K Parts and Appliances	4			
111	Pt 21 Sub Part M Repairs	13			
112	Pt 21 Sub Part O ETSO Authorization	16			
113	Pt 21 Sub Part Q Identification of Products	6			
114	*Design and Production*	*2*			
115	*Type Certificate*	*2*			
116	*Airworthiness Certificate*	*2*			
117	*ETSO*	*2*			
118	*Pt 21 Regulation*	*2*	754	18	118/33
	Pt 21 Related PDS issues				
119	Ac Design	8			
120	R and M Tests	4			
121	Production	2			
122	Product	4			
123	Maintenance Manuals	8			
124	Product Training	4			
125	OEM Spares	6			
126	*Pt 21 Product Support*	*2*			
127	*Pt 21 Pt M Interface*	2	794	9	127/35
	Pt M AO Performance				
128	Pt M Sub Part B Accountability	3			
129	Pt M Sub Part C CAW	8			
130	Pt M Sub Part D Maintenance Standards	4			
131	Pt M Sub Part E Components	5			
132	Pt M Sub Part G CAMO	14			
133	Pt M Sub Part H CRS	3			
134	Pt M Sub Part I Airworthiness Review	6			
135	Pt M Pt145 Contract Interface	9	843	8	135/35
	Pt 145 Performance				
136	Pt145 Org Performance	19			
137	Maintenance Data	12			
138	GSE	14			
139	Tools And Test Equipment	14			
140	LRU Spares	10			
141	Facility Environment	17			
142	*Logistic Support*	2			
143	Task Management Documents	6			
144	Manning	5	942	9	144/36

	Individual Performance				
145	Attitude to Task	7			
146	Work-face Stress	7			
147	Task	13			
148	Competence	2			
149	Continuation training	5			
150	Tech Knowledge Skills	8			
151	Certification and Re-certification	5			
152	Physiological limits	6			
153	Physical health	8			
154	Personal Stress	4			
155	*Health and Welfare*	*2*			
156	*Individual traits*	*2*	1011	12	156/38
	Licensing Authority				
157	Training and Qualification	7			
158	Health Fitness	3			
159	Part 66 Licensing	7	1028	3	159/38
	CAW Consolidation				
160	*Pt 145 Performance*	*2*			
161	*Part M Org*	*2*			
162	*CAW Management*	*2*	1034	3	162/41
	Defences and Consequences				
163	Defences at Pt145	3			
164	Consequences at Pt145	4			
165	*Release to Fly*	*2*			
166	Defences at Pt M	3			
167	Consequences at Pt M	4			
168	*Handling & Despatch*	*2*			
169	Defences at H & D	3			
170	Consequences at H & D	4			
171	Defences at Pre TO	3			
172	Consequence at Pre TO	5			
173	*Take Off*	*2*			
174	Flight and Consequences	7			
175	Combined Cost	11	1087	13	175/44
	Added for validation trial				
176	Pt 21_Pt M Product Support Contract	9			
177	Defence Quality	3			
178	Consequence Quality	5	1104	3	178/44

	Air Cargo subset				
179	Cargo	6			
180	Cargo Loading	8			
181	Loading Conditions (Environmental)	11			
182	*Cargo and Role Equipment*	*2*			
183	Defence Cargo & Role Equipment	3			
184	Consequence Cargo	4	1138	6	184/45

Intentionally Blank

Appendix 11

MEDA taxonomy versus CAW Risk Model taxonomy

This appendix provides information on the extent of coverage of MEDA Form taxonomy with CAW Risk Model's taxonomy.

Serial No	MEDA Parameter	CAW Risk Model Equivalent
1	Section 1. Event Identification	Operation Vs Capability subsystem, Management information nodes
2	Section 2. Event	Operational effect of the detected error, accommodated under the sub system Consequences
3	Section 3 – Maintenance Error	Type of maintenance error or type of damage to equipment tools or personal injury error. These are not CF and so could be covered under management information in a future development of the risk model but not currently covered.
	Section 4	
4	A. Information Work Cards	Covered under Subsystem Pt 21 Performance/ node Maintenance Manuals and Pt 145 Performance Sub System/ node Maintenance Data.
5	B. Equipment Tools Safety Equipment	All 3rd tier CFs have been accommodated in Pt 145 Performance under nodes GSE and node Tools and Test Equipment
6	C. Aircraft Design/ Configuration/ Parts	These have been shared between Pt 21 Performance /under node Design and node OEM Spares
7	D. Job/ Task.	All five, 3rd tier CF have been accommodated under Pt 145 Performance/ node Attitude to Task.
8	E. Technical Knowledge/ Skills.	All the 3rd tier CFs have been identified in Pt 145 Performance/ Personnel Group, Certification and Training, nodes for Training and Qualification, and Technical Knowledge and Skills
9	F Individual factors.	F1, 2, 6, 7, 9 (physical health, fatigue, body strength, personal event, memory lapse) all these have been taken into account under Pt 145 Performance Individual Traits and nodes Physiological Limit, Physical health and Personal Stress. The remainder is covered under Pt 145 Work Face Stress and Attitude to Task.
10	G. Environmental/ Facilities.	All points covered by Pt 145 Performance Environment/ Facilities node.
	H. Organizational Factors.	These are covered as follows.
11	H1. Quality of support from technical organizations, e.g. engineering, planning and technical pubs.	Quality of the organization has been represented in MEDA Form as a one line. Quality is an underpinning issue for the technical welfare of the entire organization; it is a complex factor and needed a greater resolution as well as a greater critical analysis. Accordingly, quality has been allocated a separate QMS subsystem, and the factors have been further decomposed into smaller elements.
12	H2. Company policies.	MEDA defines this as a one line. It is one of the most important factors on which the organization is pivoted on. In CAW risk model a separate subsystem "Corporate Policy" and 7 nodes (each decomposed into several 3rd tier causal factors) have been provisioned to capture Organization's Corporate Policy related causal factors.

13	H3. Not enough staff.	This single line item has been covered under Pt 145 Performance, Manning node. It provides a higher resolution, lack of trade cover, supervision etc.
14	H4. Corporate Change/ Restructuring.	Under the title "Change Management" this single line 3rd tier item has been allocated a full stand alone subsystem and 6-nodes, each with several 3rd tier causal factors. There is a greater resolution enabling more complex situations to be recorded.
15	H5. Union Action.	Trade Union influence as a factor has been accommodated as an external input affecting "Corporate policy" and is given its own node "Trade Union" with several 3rd tier causal factors.
16	H6. Work process/ Procedure.	Pt 145 Performance Node Task Management Docs or Pt 21 Performance Node Maintenance Manuals. CAW risk model offers a greater resolution
17	H7. Work process/ procedure not followed.	Listed under Task Node, approved data not followed.
18	H8. Work process/ procedure not documented.	Listed under Task Node, Unrecorded work.
19	H9. Work group normal practice (norm).	This item has not been catered in the model. Perhaps we should add that.
20	H10. Others	Covered by numerous other nodes and causal factors in CAW risk model.
21	I. Leadership and Supervision.	This Human Factors issue is part applicable to Pt M responsibility such as planning and organization of tasks, prioritization, delegation and unreasonable expectation, all of which are applicable to the planning stage of tasks and contracting out. In MEDA it is more relevant to individual practical tasks allocated to individuals or groups of people (section or team). In the case of Pt M Performance, the requirements is covered under Pt M Performance, Nodes Pt M Sub Part D Maintenance Standards (MA 402 Maintenance Performance) and Part M Sub Part G CAMO (MA 706 (personnel), 707 (staff) and 708 (CAW management). In the case of Pt 145, presently covered under Pt 145 A30-Competency of Personnel and Supervisory staff. Leadership and Supervision and the skills of doing management tasks should be part of this competency.
22	J. Communication.	This is another Human factors issue that is often breached. Communications is one of the very important issues. There should be a separate node for it under Pt 145 performance and could be provided in a development model.
23	Duplication of MEDA 3rd tier causal factors.	Some MEDA 3rd tier causal factors (CF) may have been duplicated under different nodes in the CAW Risk Model. This is to ensure that multiple errors relating to a single incident could be accommodated.

Appendix 12

Taxonomy for the CAW Risk Model

This Appendix provides details of the taxonomy used for the CAW Risk Model. The names have been coded to match with the names used in the model. They are self-explanatory; names of sub divisions (causal factors) indicate the significance of the node. Generic names have been used in some cases, e.g. Aircraft Type A1 is generic to be assigned to a Boeing 747 and Version, or an Airbus 340 and Version etc, whatever the types and versions that an operator may be utilizing. Individual user may select and assign types to names to suit their circumstances; unused names should be deleted from the model.

Names are grouped under subsystems or groups of nodes; the top row has been colour coded to facilitate tracking.

Operation Vs Capability

Aircraft_Type_Series_FW	Aircraft_Type_Series_RW	Registration_No	AC_Age	Sectors_Flown	Maj_Maintenance_Cycles	Ac_Generation_Time
No_Error	No_Error	No_Error	No_Error	No_Error	No_Error	No_Error
Type_A1	Type_H1	Reg_1	Upto_5yr	Under_5000	Under_1	Planned_Average
Type_A2	Type_H2	Reg_2	Over5_to_10yr	Over5000_to_10000	Over1_to_2	Shorter_than_Average
Type_A3	Type_H3	Reg_3	Over10_to_15yr	Over10000_to_15000	Over2_to_3	Longer_than_Average
Type_B1	Type_J1	Reg_4	Over15_to_20yr	Over15000_to_20000	Over3_to_4	
Type_B2	Type_J2	Reg_5	Over20_to_25yr	Over20000_to_25000	Over4_to_5	
Type_B3	Type_J3	Reg_6	Over25_to_30yr	Over25000_to_30000	Over5_to_6	
Type_C1	Type_K1	Reg_7	Over30_to35yr	Over30000_to_35000	Over6_to_7	
Type_C2	Type_K2	Reg_8	Over35_to_40yr	Over35000_to_40000	Over7_to_8	
Type_C3	Type_K3	Reg_9	Over40_to_45yr	Over40000_to_45000	Over8_to_9	
Type_D1	Type_L1	Reg_10	Over45_to_50yr	Over45000_to_50000	Over9_to_10	
Type_D2	Type_L2	Reg_11				
Type_D3	Type_L3	Reg_12				

Aircraft	Operating_Role	Route	Nature_of_Operation	Flight_Origin	Destination
No_Error_Probability	No_Error	No_Error	No_Error_Probability	No_Error	No_Error
Error_Probability	Pax_legacy	Long_haul	Error_Probability	Western_Europe	Western_Europe
	Pax_tour_op	ETOPS		Eastern_Europe	Eastern_Europe
	Pax_commuter	Medium_range		CIS	CIS
	Pax_regional_value	Short_range		US_Canada	US_Canada
	Pax_LowCost			Central_South_America	Central_South_America
	Pax_charter			South_Africa	South_Africa
	Cargo			North_Africa	North_Africa
	Combi			Central_Africa	Central_Africa
				Mid_East	Mid_East
				South_Asia	South_Asia
				Asia_Pacific	Asia_Pacific
				Japan	Japan
				China_Far_East_Asia	China_Far_East_Asia

Departure_Time	Geo_Location_Time	FleetSize_to_TR_Cat_A_Staff	FleetSize_to_TR_Cat_B1_Staff	FleetSize_to_TR_Cat_B2_Staff
No_Error	No_Error_Probability	No_Error	No_Error	No_Error
Local_0000_0159H	Error_Probability	To_Scale	To_Scale	To_Scale
Local_0200_0359H		Better_than_Scale	Better_than_Scale	Better_than_Scale
Local_0400_0559H		Worse_than_Scale	Worse_than_Scale	Worse_than_Scale
Local_0600_0759				
Local_0800_0959H				
Local_1000_1159H				
Local_1200_1359H				
Local_1400_1559H				
Local_1600_1759H				
Local_1800_1959H				
Local_2000_2159H				
Local_2200_2359H				

FleetSize_to_TR_Cat_C_Staff	FleetSize_to_NonCat_Tech_Staff	Tech_Staff	FleetSize_to_Logs_Staff	FleetSize_to_Tech_Managers
No_Error	No_Error	No_Error_Probability	No_Error	No_Error
To_Scale	To_Scale	Error_Probability	To_Scale	To_Scale
Better_than_Scale	Better_than_Scale		Better_than_Scale	Better_than_Scale
Worse_than_Scale	Worse_than_Scale		Worse_than_Scale	Worse_than_Scale

Other_Support_Staff	Staff_Complement	Operation_Vs_Capability
No_Error_Probability	No_Error_Probability	No_Error_Probability
Error_Probability	Error_Probability	Error_Probability

Pt 21 Regulation – Regulatory Compliance

Pt21_SpA_GeneralProvisions	Pt21_SpB_TypeCertificates	Pt21_SpD_ChangesTo_TC	Pt21_SpE_Supplemental_TC	Pt21_SpF_ProductionWO_POA
No_Error	No_Error	No_Error	No_Error	No_Error
Pt21A2_Undertaking_by_another	A13_Eligibility	A92_Eligibility	A112_Eligibility	A122_Eligibility
Pt21A3_FailureMalfuncDefects	A14_Demo_Capability	A93_Application	A112B_Demo_Capability	A124_Application
Pt21A3B_ADs	A15_Application	A95_MinorChanges	A113_Application_SuppTC	A125_LetterOfAgreement
Pt21A4_Coord_DesgnAndProductn	A16A_AW_Codes	A97_MajorChanges	A114_DemoCompliance	A125B_Findings
	A16B_SpeclConditions	A101_DemonstrationCompli	A115_Issuing_SuppTC	A125C_Duration_ContValidity
	A17_TC_Basis	A103_Approval	A116_Transferability	A126_ProdInspecSystem
	A18_EnvProtectionReqmnt	A105_RecordKeeping	A117_ChangestoProduct_SuppTC	A127_TestingAircarft
	A19_Changes_NewTC	A107_CAW_Instructions	A118A_Obligations_EPA_Marking	A128_TestingEngineAndProp
	A20_ComplianceWithA17_A18	A109_Obligations_EPA_Marking	A118B_Duration_ContValidity	A129_ManufacturerObligations
	A21_Issuing_TC		A119_Manuals	A130_ConformityStatement
	A23_Issue_Restrtd_TC		A120_CAW_Instructions	
	A31_TypeDesign			
	A33_InvestigationAndTests			
	A35_FlightTests			
	A41_TypeCertificate			
	A44_TC_Holder_Obligations			
	A47_Transferability			
	A51_Duration_ContValidity			
	A55_RecordKeeping			
	A57_Manuals			
	A61_CAW_Instructions			

Pt21_SpH_AirworthinessCert	Pt21_SpI_Noise_Certificates	Pt21_SpJ_DOA	Pt21_SpK_Parts_and_Appliances	Pt21_SpM_Repairs
No_Error	No_Error	No_Error	No_Error	No_Error
A172_Eligibility	A203_Eligibility	A233_Eligibility	A303_Compliance_Requirements	A432_Eligibility
A173_AWC_Classification	A204_Application	A234_Application	A305_ApprvlPartsAppliances	A432B_Capability_Demo
A174_Application	A205_Issue_of_Noise Cert	A235_IssueDOA	A307_ReleasePartsAppl	A433_RepairDesign
A175_Language	A207_Amendments_Mods	A239_DesignAssuranceSystem		A435_RepairClassification
A177_Amendments_Mods	A209_Transferability_Reissue	A243_Exposition_Data		A437_IssueRepairDesignApproval
A179_Transferability_Reissue	A210_InspectionAccess	A245_DemoApprovalReqmnt		A439_RepairPartsProduction
A180_InspectionAccess	A211_Duration_ContValidity	A247_ChangesToDes_Assu_Sys		A441_RepairEmbodiment
A181_Duration_ContValidity		A249_Transferability		A443_Limitations
A182_Ac_Identification		A251_TermsOfApproval		A445_UnrepiredDamage
A183_Issuing_AW_Cert		A253_ChangesToTOA		A447_RecordKeeping
A184_Issuing_Restrd_AW_Cert		A257_Investigations		A449_CAW_Instructions
A185_Issuing_Permit_to_Fly		A258_Findings		A451_Obligations_EPA_Marking
		A259_Duration_ContValidity		
		A263_Privileges		
		A265_ObligationsOfPOAHolder		

Pt21_SpO_ETSO_Authoriztn	Pt21_SpQ_IdentifictnProducts	Design_and_Production	Type_Certificate	Airworthiness_Certificate
No_Error	No_Error	No_Error_Probability	No_Error_Probability	No_Error_Probability
A602A_Eligibility	A801_IdentificProducts	Error_Probability	Error_Probability	Error_Probability
A602B_DemoCapability	A803_HandlingIdentData			
A603_Application	A804_IndentfyPartsAppliances			
A604_ETOAuthorizatn	A805_IdentOfCriticalParts			
A605_ExpositionAndData	A807_IdentETSOArticles			
A606_IssueETSOAuthorizatn				
A607_ETSOAuthoriznPrivileges				
A608_DeclOfDesignAndPerform				
A609_ObligationsOfETSOHolders				
A610_DeviationsApproval				
A611_DesignChanges				
A613_RecordKeeping				
A615_InspectionAccess				
A619_Duration_ContValidity				
A621_Transferability				

ETSO	Pt21_Compliance
No_Error_Probability	No_Error_Probability
Error_Probability	Error_Probability

Part 145 –
Regulatory Compliance

Part_145_AO_Findings_L1	Part_145_AO_Findings_L2
No_Error	No_Error
A20_Terms_of_approval	A20_Terms_of_approval
A25_Facilities	A25_Facilities
A30_Personnel	A30_Personnel
A35_Certifying_and_suppt_staff	A35_Certifying_and_suppt_staff
A40_Tooling_Material_Eqpt	A40_Tooling_Material_Eqpt
A42_Acceptance_of_components	A42_Acceptance_of_components
A45_Maintenance_data	A45_Maintenance_data
A47_Production_planning	A47_Production_planning
A50_Certification_of_maintenan	A50_Certification_of_maintenan
A55_Maintenance_records	A55_Maintenance_records
A60_Occurrence_reporting	A60_Occurrence_reporting
A65_Safety_and_Quality	A65_Safety_and_Quality
A70_MOE	A70_MOE
A75_Privileges	A75_Privileges
A80_Limitations_of_AO	A80_Limitations_of_AO
A85_Changes_to_AO	A85_Changes_to_AO
A90_Continued_validity	A90_Continued_validity
A95_Findings	A95_Findings

Compliance_145
No_Error_Probability
Error_Probability

Part M-
Regulatory Compliance

PtM_SpB_Findings_L1	PtM_SpB_Findings_L2
No_Error	No_Error
MA201_Responsibilities	MA201_Responsibilities
MA202_Occurrence_Reporting	MA202_Occurrence_Reporting

PtM_SpB_Compliance	PtM_SpC_Findings_L1	PtM_SpC_Findings_L2	PtM_SpC_Compliance	PtM_SpD_Findings_L1
No_Error_Probability	No_Error	No_Error	No_Error_Probability	No_Error
Error_Probability	MA301_CAW_tasks	MA301_CAW_tasks	Error_Probability	MA401_Maintenance_Data
	MA302_Ac_Maintenance_Program	MA302_Ac_Maintenance_Program		MA402_Maintenance_Performance
	MA303_AW_Directives	MA303_AW_Directives		MA403_Ac_Defects_Rectification
	MA304_Mods_and_Repair_Data	MA304_Mods_and_Repair_Data		
	MA305_Ac_CAW_Record_System	MA305_Ac_CAW_Record_System		
	MA306_Operator_Tech_Log_System	MA306_Operator_Tech_Log_System		
	MA307_Transfer_of_CAW_records	MA307_Transfer_of_CAW_records		

PtM_SpD_Findings_L2	PtM_SpD_Compliance	PtM_SpE_Findings_L1	PtM_SpE_Findings_L2	PtM_SpE_Compliance
No_Error	No_Error_Probability	No_Error	No_Error	No_Error_Probability
MA401_Maintenance_Data	Error_Probability	MA501_Installation	MA501_Installation	Error_Probability
MA402_Maintenance_Performance		MA502_Component_maintenance	MA502_Component_maintenance	
MA403_Ac_Defects_Rectification		MA503_Life_limited_components	MA503_Life_limited_components	
		MA504_Control_of_US_components	MA504_Control_of_US_components	

PtM_SpG_Findings_L1	PtM_SpG_Findings_L2	PtM_SpG_Compliance	PtM_SpH_Findings_L1	PtM_SpH_Findings_L2
No_Error	No_Error	No_Error_Probability	No_Error	No_Error
MA704_CAM_Exposition	MA704_CAM_Exposition	Error_Probability	MA801_Ac_CRS	MA801_Ac_CRS
MA705_Facilities	MA705_Facilities		MA802_Component_CRS	MA802_Component_CRS
MA706_Personnel_requirements	MA706_Personnel_requirements			
MA707_CAW_review_staff	MA707_CAW_review_staff			
MA708_CAW_management	MA708_CAW_management			
MA709_Documentation	MA709_Documentation			
MA710_Airworthiness_review	MA710_Airworthiness_review			
MA711_CAMO_privileges	MA711_CAMO_privileges			
MA712_Quality_system	MA712_Quality_system			
MA713_Changes_to_CAW_orgnzn	MA713_Changes_to_CAW_orgnzn			
MA714_Record_keeping	MA714_Record_keeping			
MA715_Validity_of_approval	MA715_Validity_of_approval			
MA716_Findings	MA716_Findings			

PtM_SpH_Compliance	PtM_SpI_Findings_L1	PtM_SpI_Findings_L2	PtM_SpI_Compliance
No_Error_Probability	No_Error	No_Error	No_Error_Probability
Error_Probability	MA901_Ac_airworthiness_review	MA901_Ac_airworthiness_review	Error_Probability
	MA902_Validity_of_ARC	MA902_Validity_of_ARC	
	MA903_Transfer_of_ac_within_EU	MA903_Transfer_of_ac_within_EU	
	MA904_AW_review_EUimportedAC	MA904_AW_review_EUimportedAC	
	MA905_Findings	MA905_Findings	

Compliance_M	Pt145_PtM_Compliance
No_Error_Probability	No_Error_Probability
Error_Probability	Error_Probability

Pt 21 Performance

Ac_Design	RandM_Tests	Production	Product	Maintenance_Manuals	Product_Training
No_Error	No_Error	No_Error	No_Error	No_Error	No_Error
Design_Error	RandM_Tests_bypassed	Production_Faults	Design_issues	Incomprehensible	Maintainability_issue
Missed_Design_Review	RandM_Tests_inexact		Production_issues	Tech_info_unavailable	New_Technology_transfer
Complex	RandM_Tests_unsatis		RandM_issues	Incorrect	TTE_undefined
Inaccessible				Conflicting	
Variable_Ac_Config				Unsatis_update_process	
Easy_to_install_incorrectly				Incorrectly_modified_AMM	
Other				Ambiguous	

OEM_Spares	Pt21_ProductSupport	Pt21_PtM_ProdSupp_Contract	Pt21_PtM_Interface
No_Error	No_Error	No_Error	No_Error_Probability
Complex	Error	Management	Error_Probability
Parts_unavailable		Contract_conditions_unsatis	
Parts_incorrect_label		Poor_funding	
Easy_to_install_incorrectly		Engineering_support	
Other		Defect_investigation	
		Spares_Supply_Chain	
		Product_Training	
		Docs_support	

Pt M Performance

PtM_SpB_Accountability	PtM_SpC_Cont_Airworthiness	PtM_SpD_Maintenance_Standards	PtM_SpE_Components
No_Error	No_Error	No_Error	No_Error
MA201_Responsibilities	MA301_CAW_tasks	MA401_Maintenance_Data	MA501_Installation
MA202_Occurrence_Reporting	MA302_Ac_Maintenance_Program	MA402_Maintenance_Performance	MA502_Component_maintenance
	MA303_AW_Directives	MA403_Ac_Defects_Rectification	MA503_Life_limited_components
	MA304_Mods_and_Repair_Data		MA504_Control_of_US_components
	MA305_Ac_CAW_Record_System		
	MA306_Operator_Tech_Log_System		
	MA307_Transfer_of_CAW_records		

PtM_SpG_CAMO	PtM_SpH_CRS	PtM_SpI_Airworthiness_review	PtM_Pt145_Contract_IntFace
No_Error	No_Error	No_Error	No_Error
MA704_CAM_Exposition	MA801_Ac_CRS	MA901_Ac_airworthiness_review	Management
MA705_Facilities	MA802_Component_CRS	MA902_Validity_of_ARC	Contract_conditions_unsatis
MA706_Personnel_requirements		MA903_Transfer_of_ac_within_EU	Task_definition
MA707_CAW_review_staff		MA904_AW_review_EUimportedAC	Quality_control
MA708_CAW_management		MA905_Findings	Engineering_support
MA709_Documentation			Spares_Supply_Chain
MA710_Airworthiness_review			Product_Training
MA711_CAMO_privileges			Docs_support
MA712_Quality_system			
MA713_Changes_to_CAW_orgnzn			
MA714_Record_keeping			
MA715_Validity_of_approval			
MA716_Findings			

Pt 145 Performance

Pt145_Org_Performance	Maintenance_Data	GSE	ToolsAndTestEqpt	LRU_Spares
No_Error	No_Error	No_Error	No_Error	No_Error
A20_Terms_of_approval	Poor_access_to_data	Unsafe	Unsafe	Complex
A25_Facilities	Unavailable_at_workface	Unreliable	Unreliable	Inaccessible
A30_Personnel	Info_not_used	Poor_ControlLayout_display	Poor_ControlLayout_display	Variable_ac_config
A35_Certifying_and_suppt_staff	Incomprehensible	MisCalibrated	MisCalibrated	Parts_unavailable
A40_Tooling_Material_Eqpt	Tech_info_unavailable	Unavailable	Unavailable	Parts_incorrect_label
A42_Acceptance_of_components	Incorrect_data	Inappropriate	Inappropriate	Easy_to_install_incorrectly
A45_Maintenance_data	Confliciting_data	Mismatch_environment	Mismatch_environment	Faulty_PMA_part
A47_Production_planning	Not_updated	No_instructions	No_instructions	Rogue_Part
A50_Certification_of_maintenan	Incorrect_amendment	Too_complicated	Too_complicated	Other
A55_Maintenance_records	Ambiguous	Incorrect_label	Incorrect_label	
A60_Occurrence_reporting	Confusing_graphics	Not_used	Not_used	
A65_Safety_and_Quality		Incorrectly_used	Incorrectly_used	
A70_MOE		Other	Other	
A75_Privileges				
A80_Limitations_of_AO				
A85_Changes_to_AO				
A90_Continued_validity				
A95_Findings				

Facility_Environment	Logistic_Support	Task_Managmnt_Docs	Manning	Attitude_to_Task	Workface_Stress
No_Error	No_Error_Probability	No_Error	No_Error	No_Error	No_Error
Noise	Error_Probability	Definition	Trade_cover	Repetitive_monotonous	Time_constraint
Hot		Instructions	Supervision	Complex_confusing	Peer_pressure
Cold		Inaccessible	Certification	New_task_Task_change	Poor_Teamwork
Humid		Info_not_used	Coordination	Different_from_other_similar	Physical_stress
Rain		Illegible		Complacent	Personal_stresses
Snow				Others	Fatigue_Sleeplessness
Lighting					
Wind					
Vibration					
Cleanliness					
Hazard_toxic_substances					
Power_source					
Ventilation					
Markings					
Husbandry					
Other					

Task
No_Error
Installation_error
Apprvd_data_not_followed
Poor_inspection_standard
Servicing_error
Poor_maintenance_practice
Misinterpretation_of_data
Inattention_damage
Missed_independent_checks
Unrecorded_work
Work_uncertified
Certified_without_verification

Certification and Rating

Training_and_Qualification	Health_Fitness	Part_66_Licensing	Competence
No_Error	No_Error	No_Error	No_Error
Knowledge	Poor_health_undeclared	Documentation	Lack_competence
Skills	Poor_fitness_undeclared	Training	
Practical_skills		Testing	
On_aircraft_skills		Achivements	
Documentation_procedures		Health	
Integrity		Integrity	

Cont_Training	Tech_Knowldg_Skills	Certification_Recert
No_Error	No_Error	No_Error
Training_program	Type_training	Type_rating
Non_or_poor_Attendance	Task_knowledge	Certified_but_inexperienced
Poor_content	Task_planning	Experienced_but_uncertified
Poor_instruction	Ac_system_knwldg	Uncertified_inexperienced
	Airline_process_knwldg	
	English_lang_prof	
	Other	

Personal Traits

Physiological_Limits	Physical_Health	Personal_Stress	Health_and_Welfare	Individual_Traits
No_Error	No_Error	No_Error	No_Error_Probability	No_Error_Probability
Body_size	Physically_ill	Personal_event	Error_Probability	Error_Probability
Reach_or_grip	On_medication	Domestic_or_financial_issues		
Strength	Fatigue	Natural_low_stress_threshold		
Colour_perception	Impaired_Visual_perception			
Limited_mobility	Impaired_Hearing			
	Memory_lapse			
	Mobility_impaired			

Quality Management

CAW_Quality_Policy	Quality_Plan_and_Program	QA_Scope	Resources_and_TrngStandards	Audit_Procedure
No_Error	No_Error	No_Error	No_Error	No_Error
QS_Objective	Areas_to_be_Audited	Quality_System	Resource_Level	Prescribed_Procedures
Defn_Standards_References	Reference_Rationale	Air_Safety_and_MOR	Independence_of_Auditors	Details_of_processes
	Sampling_Frequency	CAME_Organzn	Direct_Access_to_AM	QA_Process_Details
	Audit_Time_Frame	Technical_Log	Direct_Access_to_Operator	Report_Format
	Nominated_Auditor	CAW_Management	Access_to_Subcontractor	Distrbutn_Reports
		Planning_and_Tech_Rec	Auditor_Qualifications	Remedial_Actions
		Base_Maintenance	Auditor_AC_Experience	SubContractor_Audit
		Line_Stations	Training_Standard	Supplier_Auditing
		Aircraft_in_Service		
		Fuel_Provisions		
		De_Anti_Icing_Provisions		
		Engine_Off_Wg_Maintenance		
		APU_Off_Wg_Maintenance		
		UC_Off_AC_Maintenance		

Remedial_Action_Procedure	CAW_Management_Activity	Monitor_Effectiveness_of_AMP	MaintenanceContract_Monitoring
No_Error	No_Error	No_Error	No_Error
Reporting_Findings	Pt_MA_SubPt_C_Tasks	Periodic_Effectiveness_Reviews	Contract_Agreement
Corrective_Action_Procedure	Management_AMP_and_RP	Identify_SetUp_Procedures	Defined_Standards_Regs
Correct_NonConformalities	Management_AMP_RP_Amendments		Deliverables
Review_Actions	Management_Mods_and_Repairs		Indivls_Awareness_of_Terms
Evaluation	Maintenance_IAW_AMP_PtM_SubPtH		Compliance_Oversight_of_AMO
	Management_AD_and_OD		Contracted_AMO_Apprvl_Review
	Management_Reported_Defects		AF_Engine_Comp_Coverage
	Maintenance_by_Approved_AMO		Organizational_Feedback
	Coord_AMP_AD_LifeItems_ComInsp		Contractual_Amendments
	Manage_Permitted_Variations		

QMS_Policy_Plans_Scope	QMS_Tasks_Processes	QMS_Organization	PtM_Management_Activity	PtM_Finding_Reporting
No_Error_Probability	No_Error_Probability	No_Error_Probability	No_Error	No_Error
Error_Probability	Error_Probability	Error_Probability	Interface_Contract	Finding_1
			Pt_MA_SubPt_C_Tasks	Finding_2
			Management_AMP_and_RP	Observation
			Management_AMP_RP_Amendments	
			Management_Mods_and_Repairs	
			Maintenance_IAW_AMP_PtM_SubPtH	
			Management_AD_and_OD	
			Management_Reported_Defects	
			Maintenance_by_Approved_AMO	
			Coord_AMP_AD_LifeItems_ComInsp	
			Manage_Permitted_Variations	

PtM_Corrective_Action	Part_M_QA_Performance	Pt145_Activity_Area	Pt145_Finding_Reporting	Pt145_Corrective_Action
No_Error	No_Error_Probability	No_Error	No_Error	No_Error
FeedBack_on_Corrective_Action	Error_Probability	Interface_Contract	Finding_1	FeedBack_on_Corrective_Action
Actions_Review		MOE	Finding_2	Actions_Review
Evaluation		Air_Safety_and_MOR	Observation	Evaluation
		Technical_Log		
		CAW_Management		
		Planning_and_Tech_Rec		
		Base_Maintenance		
		Line_Stations		
		Aircraft_in_Service		
		Fuel_Provisions		
		De_Anti_Icing_Provisions		
		Engine_Off_Wg_Maintenance		
		APU_Off_Wg_Maintenance		
		UC_Off_AC_Maintenance		

Part_145_QA_Performance	SubContractor_Activity_Area	SC_Finding_Reporting	SC_Corrective_Action	SubContractor_QA_Performance
No_Error_probability	No_Error	No_Error	No_Error	No_Error_Probability
Error_Probability	Interface_Contract	Finding_1	FeedBack_on_Corrective_Action	Error_Probability
		Finding_2	Actions_Review	
		Observation	Evaluation	

Supplier_Activity_Area	Supplier_Finding_Reporting	Supplier_Corrective_Action	Supplier_QA_Performance	QA_Performance	Quality_Management_System
No_Error	No_Error	No_Error	No_Error_Probability	No_Error_Probability	No_Error_Probability
Interface_Contract	Finding_1	FeedBack_on_Corrective_Action	Error_Probability	Error_Probability	Error_Probability
	Finding_2	Actions_Review			
	Observation	Evaluation			

Corporate Policy

Global_Factors	Central_Government	Local_Government	Corporate_Board	Trade_Union
No_Error	No_Error	No_Error	No_Error	No_Error
ICAO	Corporate_Business_policies	Environment_Regs	Business_Strategy	Industrial_Relations_Strategy
EASA	Transport_Policy	Noise_Regs	Asset_Resources_Management	Pay_and_Conditions
FAA	Environment_Policy	Flight_Path	Business_Priortities	Health_and_Welfare
IATA	Labour_Employment_Policies	Operating_Hours	Funding	Security_of_Employment
Technology_Advancement	Education_Vocational_Training		Prestige_Publicity	Education_Training
Global_Customer_Behav	Taxation		Response_to_HL_Inputs	Specialist_Industrial_Issues
Cargo_Traffic_Variation			Profits_Loss_Management	Liabilities
Monetary_Fluctuations			Labour_Relations	Management_Interface
Fuel_Costs			Liabilities	
Political_Changes			CEO_AM_Interface	
War				
Terrorism				

CEO_AM_Decisions
No_Error
Commerical_Business
Flight_Operations
Engineering
Flight_Safety
Funding
Change_Management
Board_Level_Interface

Commercial_Policies
No_Error
Commerce_FltOPs_Interface
Commerce_Eng_Interface
Commerce_HR_Interface
Outsourcing
Contracts

Flt_Ops_Policies
No_Error
FltOps_EngOPs_Interface

Eng_Ops_Policies
No_Error
Regulatory_Compliance
Safety_Health_Quality_Polciies
FltOps_Interface
Logistic_Support_Interface
HR_Interface
Commercial_Interface

Logistic_Support_Policies
No_Error
Facilities
Manning
Equipment_provisioning
Outsourcing
Job_evaluation
Standard_times
Scaling_reviews

HR_Policies
No_Error
Recruiting
Internal_training
Pay_and_Conditions
Career_Development
Health_and_Welfare
Retirement_Pensions
Off_Duty_Employents
Industrial_Relations

Corporate_and_Policy_Issues
No_Error_Probability
Error_Probability

Change Management

Business_Management	Operations	MOE	Engineering_and_Technology	Human_Resources	Change_Management
No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Probability
Policies	Role_Change	MA_701_CAME	Aicraft_Upgrade	Resourcing_Policy	Error_Probability
Funding_Resourcing	Route_Change	Pt_145_A70_Exposition	Engine_Upgrade	OutSourcing	
Organization	Fleet_size	FAA_FAR_Pt145_Rep_Stn	Avionics_Upgrades	Recruiting	
Infrastructure	Pasenger_Volume	Transp_Canada_AM573MO	Systems_Upgrades	Training	
	Extra_AC_Temp_Leasing	Other_Foreign_AMO	Process__Changes	Pay_Condition	
	Load_Factor		Logistic_Support	Heath_And_Welfare	
			Manpower_and_Qualification	Off_Duty_Employment	
			Training		

Consequences and Risk

Pt_145_Performance	Part_M_Org	CAW_Management	Defence_Pt145	Conseq_Pt145	Defence_Quality
No_Error_Probability	No_Error_Probability	No_Error_Probability	No_Error	No_Error	No_Error
Error_Probability	Error_Probability	Error_Probability	ErrorDetected	NoEffect_ErrorCF	Error_Missed
			ErrorMissed	NoEffect_ErrorInvRectfd	Error_Detected
				FltDelay_ErrorInvRectfd	

Release_to_Fly1	Defence_PtM	Conseq_PtM	Handling_Despatch	Defence_HandD	Conseq_HandD
No_Error_Probability	No_Error	No_Error	No_Error_Probability	No_Error	No_Error
Error_Probability	ErrorDetected	NoEffect_ErrorCF	Error_Probability	ErrorDetected	NoEffect_ErrorCF
	ErrorMissed	NoEffect_ErrorInvRectfd		ErrorMissed	NoEffect_ErrorInvRectfd
		FltDelay_ErrorInvRectfd			FltDelay_ErrorInvRectfd

Conseq_Quality
No_Error
NoEffect_ErrorCF
NoEffect_ErrorInvRectfd
Rework_Repair
FltDelay_ErrorInvRectfd

Take_Off	Defence_PreTO	Conseq_PreTO	Flight_and_Consequences	Combined_Cost
No_Error_Probability	No_Error	No_Error	No_Error	No_Cost
Error_Probability	ErrorDetected	FlightDelay_RTG	Flt_Compltd_ErrorCF_NoCost	Cost_group_1
	ErrorMissed	FlightDelay_RTG_Repair	InFlt_Shutdown_Flt_Compltd	Cost_group_2
		FlightDelay_RTG_Pax_Disembark	Incidence_RTB	Cost_group_3
		LongFlightDelay_RTG_Repair_OH	Incidence_Flt_Diverted	Cost_group_4
			NonFatal_Accident	Cost_group_5
			Fatal_Accident	Cost_group_6
				Cost_group_7
				Cost_group_8
				Cost_group_9
				Cost_group_10

Air Cargo Subset

Cargo	Cargo_Loading	Loading_Conditions	Defence_CargoAndRoleEqpt	Conseq_Cargo	CargoAndRoleEqpt
No_Error	No_Error	No_Error	No_Error	No_Error	No_Error_Probability
Undeclared_DAC	Incorrect_Distribution	Time_Pressure	ErrorDetected	NoEffect_ErrorCF	Error_Probability
Aircraft_Contaminated_by_DAC	CofG_Trim_Balance_Calculation	Insuffcient_Manning	ErrorMissed	NoEffect_ErrorInvRectfd	
Escaping_Live_Animals	Faulty_Pallets	GSE_Faulty		FltDelay_ErrorInvRectfd	
Heat_Electricty_Spark_Hazard	Restraints_Inadequate	GSE_Mishandled			
Cargo_on_Fire	Moving_Loads	GSE_Vehicle_Collision			
	Damaged_Restraints	Night_Opeartion			
	Unsealed_Insecure_Container	Extreme_Cold_Weather			
		Extreme_Hot_Weather			
		Rain			
		Slippery_Surfaces			

Appendix 13

Analysis of human error incident reports – Operator X

A13.1 Background

This Appendix presents a catalogue of maintenance and CAW-process related human error incidents on aircraft operated by Operator X and on visiting aircraft to its main base, over a period of 26-months from January 2008 to Feb 2010. The incidents have been reported by either maintenance engineers or flight crews according to the circumstances of their discovery, as well as by inspectors who carried out regulatory oversight audits and internal quality audits during that period.

Operator X's aircraft operate in a wide-spread network of routes, where en-route they receive outsourced maintenance support from third party maintenance providers. Most of the aircraft have had previous owners before they joined Operator X's fleet. The aircraft receive deep maintenance, i.e. C-Checks, at MRO to whom this work has been outsourced.

Some of the errors catalogued, though they were human errors, were associated with the design or production of the aircraft, or previous owners but now owned by Operator X. Some errors have been either caused or discovered at MROs. Thus, detected errors might have been caused by Operator X's own staff, or by other personnel elsewhere during the life of these aircraft, which had remained dormant, to be surfaced during this time-period.

Incident reports have, as far as possible, ascertained where and who caused the error, and assigned the cause to the relevant source; but some had remained unanswered. Nevertheless, under the Regulation it is the current operator who is responsible for the airworthiness of their aircraft and therefore the management of continuing airworthiness process is ultimately their responsibility. All these errors have been used to determine the risk contribution to airworthiness from its CAW processes and associated organizational factors. This was the principal, more complex calculation demonstrated in the validation trial, as applicable to an AOC Holder operation.

A number of errors that were either detected or caused at the Operator X's main base facility are in this catalogue. They were maintenance and CAW related error incidents encountered at the main base on those aircraft that they had handled, and errors that were either detected or reported.

Errors discovered during quality or regulatory audits have been added to make up the full complement that was used to determine the risk contribution from each group, i.e. Operator X's main base organization or the Operator's fleet maintenance organization, to the airworthiness of aircraft that they had handled.

More about the analysis of error incidents has been explained in Chapter Eight – Validation of the Model.

A13.2 Analysis and presentation of data

In this catalogue, errors are presented in a chronological order of detection. They have been investigated and their reports closed at different dates, but not necessarily in any particular order. Serial numbers used in the catalogue are there for the researcher's reference purposes as they are linked to the original source data. Report numbers, aircraft types, registration numbers and location and individual names have been either scrambled or removed from records in order to desensitize the information for public domain use.

The catalogue presented here contains only those errors detected by operating staffs. Each error investigation report was summarised, and analyzed using a pro-forma designed for this study. In the following pages, detailed analysis of errors has been demonstrated for seven errors, Serial No: 41, 28, 18, 19, 23, 27 and 4, in that order, by providing a full set of specimen results. A presentation of all the analyzed errors in this form would be highly voluminous (estimated 7720 rows in the Tables to cover all error lines). Therefore details of the analysis of the remaining errors have been excluded from the presentation catalogue, but they can be seen in the spreadsheet in digital form, See CD/DVD – Ops X Validation Excel files.

Summaries of narrative investigation reports are included in the catalogue. Narratives of the Quality Management System Audit Findings and the Regulator Oversight Inspection Findings have been excluded from the catalogue as part of desensitizing and part to reduce the volume of this catalogue. However Findings are listed in Chapter Eight and relevant details in an analysed-form are in the database/ spreadsheet. A specimen Finding Report form (less the narrative) is included in the catalogue.

EASA Part 145 Approval Surveillance Record			(Page 1 of 8)
Organization Name		**Approval Reference**	
Survey Reference		**Date of Survey**	
Site / Aircraft		**Surveyor**	

Requirement	B Rating Audit:145.A.25 Facilities Requirements
Planning	
Objective Evidence	
Findings	

Requirement	B Rating Audit:145.A.30 Personnel Requirements
Planning	
Objective Evidence	
Findings	

EASA Part 145 Approval Surveillance Record			(Page 2 of 8)
Organization Name		**Approval Reference**	
Survey Reference		**Date of Survey**	
Site / Aircraft		**Surveyor**	

Requirement	B Rating Audit:145.A.35 Certifying Staff
Planning	
Objective Evidence	
Findings	
Requirement	B Rating Audit:145.A.40 Equipment, Tools & Material
Planning	
Objective Evidence	
Findings	

Serial No	Report No	Aircraft	Date
41	X224/**/**/***	Type_A2 G-****	1 Feb 08

Refuel valve failed to open due to a faulty relay fitted during an earlier maintenance operation.

During a refuelling operation, a fuel valve failed to open automatically; a manual reset button on the fuel panel had to be operated instead. Investigation revealed that during an earlier maintenance operation, a wrong type relay (K181 – rated for 1-sec) had been installed instead of the correct relay (rated for 5-sec). Once the correct type of relay was installed and fuel level sensor card replaced, the system tested satisfactorily.

The engineer who performed the initial relay replacement had been traced and interviewed after some considerable lapse of time. Unfortunately he was unable to elaborate on the circumstances of the previous installation except a statement to the effect that he would not have installed the old relay back, and that he would always check the received spares against the requirement/ demand to ensure that what was ordered had in fact arrived. In the absence of any further information from the engineer the report was closed.

Comments: This safety report had been raised in February 2008 but not closed until July 2009. For reasons unrecorded, there has been a long time lapse before the engineer was interviewed, but he yielded no useful information on causation. Regardless of the engineer's comments, which appear to be a statement of expected standards, the circumstances and conditions that lead to the error had been left either concealed or forgotten.

Nevertheless, the fact remains that a relay had been changed; the relevant system had malfunctioned due to the presence of a wrong type of relay in the circuit. For the purpose of modelling, the TRAX system that identified and supplied the component, as well as the engineer who placed the demand, received, checked and fitted the component remains as suspect potential source of error.

41	X224/**/**/***	Type_A2 G-****	1 Feb 08
Index	**Node Name _ Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type A2	
1.3	Registration Number	Reg 6	
1.4	Aircraft Age	Over 20 to 25yr	
1.5	Number of Sectors Flown	X	
1.6	Number of Major Maintenance Cycles	X	
1.7	Aircraft	Error Probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error Probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	****	
1.15	Geographical Location & Time	Error Probability	Combining error probability from nodes 1.12-1.14
1.26	Operation V Capability	Error Probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.5	Line Replacement Units and Spares	Other	
6.7	Logistic Support	Error Probability	Combining error probability from nodes 6.2 – 6.6
6.12	Task	Installation error	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error Probability	Combining error probability from nodes 5.9, 6.12
11	**Error Probability Defences and Consequences**		
11.1	CAW Management	Error Probability	Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145	Error Detected	
11.3	Consequences Pt 145	No Effect Error Investigated and Rectified	
11.14	Combined Cost	Cost group 3	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14

Serial No	Report No	Aircraft	Date
28	X91/**/**/***	Type_B1 OO-***	30 Sep 08

LRU incorrect part number on operator's tag (i.e. on the serviceable label attached to the component)

An LRU that had been sent away to the depot for repair had been upgraded during repair. A new part number had been stamped and reissued with a label stating the new part number. However on the return of LRU back to sender, it had been booked into the store quite unknowingly under the old part number, and then reissued against the aircraft OO-*** as an old part number item.

The engineer who was to fit the LRU had mindfully checked the part number against the voucher when he had discovered the error which the stores personnel who handled the component up to that pint had failed to detect.

If the LRU got installed without checking, configuration of the aircraft would have been compromised.

MEDA investigation had revealed that the depot had correctly identified the product with the new part number stamped on the component and on the documentation.

The error was committed when the LRU was booked into the store on its return from the repair depot.

Comments: This pro-active case demonstrates how one person's error could be negated by another person's vigilance and defence at the workface, thereby eliminating a potential flight safety risk.

As part of preventive measure for future, Supply Manager had sent out a reminder and verbally briefed all stores personnel. Individual stores personnel who handled the receipt and dispatch of this LRU had been interviewed.

28	X91/**/**/***	Type_B1 OO-***	30 Sep 08
Index	**Node Name _ Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type_B1	
1.2	Aircraft Type and Series Rotary Wing		
1.3	Registration Number	Reg_25	
1.7	Aircraft	Error Probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error Probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	*****	
1.15	Geographical Location & Time	Error Probability	Combining error probability from nodes 1.12-1.14
1.26	Operation V Capability	Error Probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
6	Pt 145 AO Error Performance (Active or Dormant)		
6.5	Line Replacement Units and Spares	Parts incorrect label	
6.7	Logistic Support	Error Probability	Combining error probability from nodes 6.2 – 6.6
11	Error Probability Defences and Consequences		
11.2	Defence Pt 145	Error Detected	
11.3	Consequences Pt 145	No Effect Error Investigated and Rectified	
11.14	Combined Cost	Cost group 3	Combining probability of consequences from nodes 11.3, 11.6, 11.9, 11.13, 11.14

Serial No	Report No	Aircraft	Date
18	X410/**/**/***	Type_B1. Reg No: NA	28 Nov 08

Unauthorized speed tape had been used to secure a blow out panel due to lack of a replacement spare.

Speed tape had been used to secure a blow out panel due to lack of spare panel to replace the worn out panel. The method of securing was inappropriate as the panel was left standing proud the surrounding surface and insecure.

On this converted Type_B1 aircraft the blow out panel was redundant because of a change of the system. Armed with some prior knowledge that there was a planned modification to permanently secure blow out panels by riveting, an experienced, senior engineer had taken a unilateral personal decision to undertake a speed tape repair without prior authorization. The repair undertaken was a diversion from the authorized maintenance procedure.

At the time the error was detected, the aircraft had already flown 2 sectors carrying this unauthorized repair. An authorized repair was carried out before the aircraft flew the next sector.

Comments: In this case no damage had been caused although the panel, facing high speed airflow, could have got detached in flight and caused co-lateral damage. The engineer had failed to exercise lateral thinking expected from a person of his seniority and deviated from best practice. The quality and standard of maintenance practised by the third party contractor, as well as the standards adopted by the senior engineer, is questionable.

For Error 18 and 18a – Two different sectors flown with error present			
Index	**Node Name _ Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type B1	
1.3	Registration Number	****	
1.4	Aircraft Age	**	
1.5	Number of Sectors Flown	****	
1.6	Number of Major Maintenance Cycles	*	
1.7	Aircraft	Error probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	******	
1.13	Destination	******	
1.15	Geographical Location & Time	Error Probability	Combining error probability from nodes 1.12-1.14
1.26	Operation V Capability	Error Probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
5	**Pt M AO Error Performance (Active or Dormant)**		
5.3	Pt M Sub Pt D Maintenance Standards	MA402 Maintenance Performance	
5.9	Pt M and Pt 145 Contract Interface	Quality control	
5.10	Pt M and Pt 145 Interface	Error Probability	Combining error probability from nodes 5.8 – 5.9
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.1	Pt 145 Organizational Performance	A65 Safety and Quality	Combining error probability from nodes 5.10, 9.12
6.5	Line Replacement Units and Spares	Parts unavailable	
6.7	Logistic Support	Error Probability	Combining error probability from nodes 6.2 – 6.6
6.12	Task	Poor maintenance practice	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error Probability	Combining error probability from nodes 5.9, 6.12
9	**Corporate Policy and Global Factors**		
9.6	CEO AM Decisions	Funding	
9.9	Engineering Operations Policies	Logistic support	

9.10	Logistic Support Policies	Spares provisioning	
9.12	Corporate and Policy Issues	Error probability	Combining error probability from nodes 9.7 – 9.11, 10.6
11	**Error Probability Defences and Consequences**		
11.1	CAW Management	Error Probability	Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145	Error Missed	
11.3	Consequences Pt 145	No Effect Error CF	
11.4	Release to Fly	Error probability	Combining error probability from nodes 11.1, 11.5
11.5	Defence Pt M	Error Missed	
11.6	Consequences Pt M	No Effect Error CF	
11.7	Handling and Despatch	Error probability	Combining error probability from nodes 3.26, 8.30, 9.12, 11.4, 11.8,
11.8	Defence H and D	Error Missed	
11.9	Consequence H and D	No Effect Error CF	
11.10	Defence Pre Take Off	Error Missed	
11.11	Take Off	Error probability	Combining error probability from nodes 11.7, 11.10
11.12	Consequence Pre Take Off	Error CF	
11.13	Flight and Consequences	Flt Completed Error CF No Cost	
11.14	Combined Cost	No cost	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14

For Error 18b – Error detected and repaired before this sector was flown

Index	Node Name _ Secondary Level	State	Tertiary Level CF
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type B1	
1.3	Registration Number	*****	
1.4	Aircraft Age	**	
1.5	Number of Sectors Flown	****	
1.6	Number of Major Maintenance Cycles	*	
1.7	Aircraft	Error probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	*****	

1.15	Geographical Location & Time	Error Probability	Combining error probability from nodes 1.12-1.14
1.26	Operation V Capability	Error Probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
5	**Pt M AO Error Performance (Active or Dormant)**		
5.3	Pt M Sub Pt D Maintenance Standards	MA402 Maintenance Performance	
5.9	Pt M and Pt 145 Contract Interface	Quality control	
5.10	Pt M and Pt 145 Interface	Error Probability	Combining error probability from nodes 5.8 – 5.9
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.1	Pt 145 Organizational Performance	A65 Safety and Quality	Combining error probability from nodes 5.10, 9.12
6.5	Line Replacement Units and Spares	Parts unavailable	
6.7	Logistic Support	Error Probability	Combining error probability from nodes 6.2 – 6.6
6.12	Task	Poor maintenance practice	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error Probability	Combining error probability from nodes 5.9, 6.12
9	**Corporate Policy and Global Factors**		
9.6	CEO AM Decisions	Funding	
9.9	Engineering Operations Policies	Logistic support	
9.10	Logistic Support Policies	Spares provisioning	
9.12	Corporate and Policy Issues	Error probability	Combining error probability from nodes 9.7 – 9.11, 10.6
11	**Error Probability Defences and Consequences**		
11.1	CAW Management	Error Probability	Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145	Error Detected	
11.3	Consequences Pt 145	No Effect Error Investigated and Rectified	
11.14	Combined Cost	Cost_group_3	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14

Serial No	Report No	Aircraft	Date
19	X423/**/**/****	Type_A2 G-****	13 Dec 08

Loose article in pneumatic couplings.

25 Hi-Lock fasteners were found resting in 2 pneumatic connectors on the aircraft used for ground services pneumatic supply. They were found by an engineer who opened up the connectors to carry out a maintenance task.

Investigations revealed that the fasteners used by another engineer on a task in the nearby freight bay structure had migrated to the pneumatic pipes because he had omitted to blank off the connectors and pipes before starting work. This is a poor husbandry issue as well as poor quality control of the maintenance task as he has not paid sufficient attention. He had no situational awareness and not mindful of the consequences of his lack of attention. Publicity has been given to the case to raise awareness amongst fellow workers.

Comments: This case primarily revolves around individual standards on husbandry and quality control of maintenance tasks. Because of the timely discovery of loose articles, there had been no flight safety consequences. Nevertheless, it brings to question the quality and safety standards practised and maintained by the third party contractor.

19	X423/**/**/****	Type_A2 G-****	13 Dec 08
Index	**Node Name _ Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type A2	
1.3	Registration Number	Reg 7	
1.4	Aircraft Age	Over25_to_30yr	
1.5	Number of Sectors Flown	****	
1.6	Number of Major Maintenance Cycles	*	
1.7	Aircraft	Error probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	******	
1.15	Geographical Location & Time	Error probability	Combining error probability from nodes 1.12-1.14
1.26	Operation V Capability	Error probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.1	Pt 145 Organizational Performance	A65 Safety and Quality	Combining error probability from nodes 5.10, 9.12
6.6	Facility and Environment	Husbandry	
6.7	Logistic Support	Error Probability	Combining error probability from nodes 6.2 – 6.6
6.12	Task	Poor maintenance practice	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error probability	Combining error probability from nodes 5.9, 6.12
11	**Error Probability Defences and Consequences**		
11.2	Defence Pt 145	Error Detected	
11.3	Consequences Pt 145	No Effect Error Investigated and Rectified	
11.14	Combined Cost	Cost group 2	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14

Serial No	Report No	Aircraft	Date
23	X28/**/**/****	Type_A2 G-****	4 Feb 09

Loose article left in the engine nacelle.

During C4 Check at the authorized MRO, when panel 611 KT, on RH (No: 2) engine pylon leading edge was opened, an aerosol lubricant can was found lodged between engine control pulley and slat drive torque tube. Markings on the can indicated that the item might have come from the stores of a satellite station (****). They were instructed to conduct a MEDA investigation.

Quality audits at the station identified the work done in the area by a mechanic of 3rd party contractor (*** Engineering) during the previous Christmas holiday period. Having completed his work in the area, the mechanic had closed the panels but failed to observe the aerosol can and to remove it during tools clearance stage. He had signed up for work as area cleared and the countersigning engineer in turn had not bothered to look over the area, on the basis of trust and confidence that he had on the mechanic.

Abnormal and adverse working conditions during Christmas holiday season had been cited as causal factors. These were: high workload and insufficient workers, poor planning of holiday work, inadequate supervision, engineer placing trust on mechanic and not taking on own responsibility to inspect the area for loose articles.

Warning letters had been issued to the mechanic and supervisor involved.

Comments: The aircraft had flown nearly 30 sectors during the period that the aerosol can remained lodged in the engine nacelle, until it was found. By chance, the can did not get dislodged by engine vibration where it could have migrated to a point where it could have fouled the adjacent cables and torque tube. There was a potential flight safety risk which, in this case, failed to materialize.

For the purpose of modelling, all sectors flown carrying the loose article hazard were input. However Flight Consequences were input as “Flight Completed_Error CF”. This was a lower end rating, whereas ICAO Definition of Risk required situations to be assessed with worst foreseeable situation. Less severe categorization was used because an assumption in categorization for this CAW Risk Model was that actual experience would be used rather than the speculation.

Error 23			
23	X28/**/**/****	Type_A2 G-****	4 Feb 09
Index	**Node Name _ Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type A2	
1.3	Registration Number	Reg 9	
1.4	Aircraft Age	Over25 to 30yr	
1.5	Number of Sectors Flown	****	
1.6	Number of Major Maintenance Cycles	*	
1.7	Aircraft	Error_Probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error_Probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	*****	L
1.15	Geographical Location & Time	Error_Probability	Combining error probability from nodes 1.12-1.14
1.16	Fleet Size to Num Cat A Staff	Worse than Scale	
1.17	Fleet Size to Num Cat B1 Staff	Worse than Scale	
1.21	Technical Staff	Error probability	Combining error probability from nodes 1.16-1.20
1.25	Staff Complement	Error probability	Combining error probability from nodes 1.121-1.24
1.26	Operation V Capability	Error_Probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.1	Pt 145 Organizational Performance	A65 Safety and Quality	Combining error probability from nodes 5.10, 9.12
6.9	Manning	Supervision	
6.11	Workface Stress	Time constraint	Combining error probability from nodes 6.9, 7.12
6.12	Task	Poor maintenance practice	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error Probability	Combining error probability from nodes 5.9, 6.12
8	**QMS Organization and Performance**		
8.17	Pt 145 Activity Area	Line Stations	
8.20	Pt 145 Quality Audit Performance	Error probability	Combining error probability from nodes 8.17 – 8.19

11	**Error Probability Defences and Consequences**		
11.1	CAW Management	Error probability	Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145	Error Missed	
11.3	Consequences Pt 145	No Effect Error CF	
11.4	Release to Fly	Error Probability	Combining error probability from nodes 11.1, 11.5
11.7	Handling and Despatch	Error Probability	Combining error probability from nodes 3.26, 8.30, 9.12, 11.4, 11.8,
11.11	Take Off	Error Probability	Combining error probability from nodes 11.7, 11.10
11.14	Combined Cost	No cost	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14
Error 23a			
Index	**Node Name _ Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type A2	
1.3	Registration Number	Reg 9	
1.4	Aircraft Age	Over 25 to 30yr	
1.5	Number of Sectors Flown	****	
1.6	Number of Major Maintenance Cycles	*	
1.7	Aircraft	Error probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	******	L
1.15	Geographical Location & Time	Error probability	Combining error probability from nodes 1.12-1.14
1.16	Fleet Size to Num Cat A Staff	Worse than Scale	
1.17	Fleet Size to Num Cat B1 Staff	Worse than Scale	
1.21	Technical Staff	Error probability	Combining error probability from nodes 1.16-1.20
1.25	Staff Complement	Error probability	Combining error probability from nodes 1.121-1.24
1.26	Operation V Capability	Error probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
6	**Pt 145 AO Error Performance (Active or Dormant)**		

6.1	Pt 145 Organizational Performance	A65 Safety and Quality	Combining error probability from nodes 5.10, 9.12
6.9	Manning	Supervision	
6.11	Workface Stress	Time constraint	Combining error probability from nodes 6.9, 7.12
6.12	Task	Poor maintenance practice	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error Probability	Combining error probability from nodes 5.9, 6.12
8	**QMS Organization and Performance**		
8.17	Pt 145 Activity Area	Line Stations	
8.20	Pt 145 Quality Audit Performance	Error probability	Combining error probability from nodes 8.17 – 8.19
11	**Error Probability Defences and Consequences**		
11.1	CAW Management	Error probability	Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145	Error Detected	
11.3	Consequences Pt 145	No Effect Error CF	
11.4	Release to Fly	Error Probability	Combining error probability from nodes 11.1, 11.5
11.14	Combined Cost	Cost group 3	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14

Serial No	Report No	Aircraft	Date
27	X80/**/**/****	Type_A2 G-****	15 Mar 09

Enhanced Ground Proximity Warning System (EGPWS) spurious warnings.

Spurious warnings from the Enhanced Ground Proximity Warning System had been reported by flight crew, which had been the subject of 9-separate flight operations safety reports. This maintenance safety report has been raised to cover the maintenance and airworthiness aspects of the same incidences.

Investigations have traced the source of spurious warnings to 6-loose connectors on the Radio Altimeter Trans/Receiver attributed to faulty workmanship by third party contractors' maintenance work undertaken during a period immediately before the incidence of spurious warnings. It had been revealed that the contractor had been tasked with the replacement of insulation blankets, for which the schedule of work called for the removal and reinstallation of equipment racks. The Rad Alt TR/RX is installed in one these racks and it would appear that during the reinstallation phase, the engineer responsible for that work had failed to properly connect up the 6-cables to the component, thereby giving rise to faulty warning indications.

MEDA investigation conducted by the Quality Audit Department of the contractor had attributed this human error in maintenance to a number of causal factors. Lack of awareness, and poor communications were the primary causes. Distractions and interruptions, lack of clarity thorough the absence of stage checks, inadequate job card layout, and certification issues have been quoted as secondary causes.

As a result, the third party contractors have put in place preventative measures to ensure that further incidents of this kind would not recur.

The operator too has made a change to the job card procedure. Removal and installation tasks for each of the 5 equipment racks have now been divided into separate stages. This provided a clearer step-by-step process, which would simplify the certification of each task and allow the work to be completed in stages if required

Comments:

1. This investigation and its outcome demonstrate the way the weaknesses of an interfacing contract could be exploited by a third party contractor, when its own maintenance standards fail. In this particular case the third part contractor had claimed that the job card layout was inadequate to micro manage a complex task, whereas the client operator assumed and expected the contractor to be knowledgeable enough of the task and competent to perform the task properly without having a detailed checklist.

2. All 9-sectors were recorded as carrying an error that missed detection, due to misdiagnosis. The risk was not realised by sheer chance, and the presence of alternative equipment to provide altitude information. This is of course a feature of a defended system.

27	X80/**/**/****	Type_A2 G-****	15 Mar 09
Index	**Node Name Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type A2	
1.3	Registration Number	Reg 9	
1.4	Aircraft Age	Over 25 to 30yr	
1.5	Number of Sectors Flown	****	
1.6	Number of Major Maintenance Cycles	*	
1.7	Aircraft	Error Probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error Probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	*****	
1.15	Geographical Location & Time	Error Probability	Combining error probability from nodes 1.12-1.14
1.26	Operation V Capability	Error Probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
5	**Pt M AO Error Performance (Active or Dormant)**		
5.9	Pt M and Pt 145 Contract Interface	Quality control	
5.10	Pt M and Pt 145 Interface	Error Probability	Combining error probability from nodes 5.8 – 5.9
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.1	Pt 145 Organizational Performance	A50 Certification of maintenance	Combining error probability from nodes 5.10, 9.12
6.8	Task Management Documents	Definition	
6.9	Manning	Coordination	
6.10	Attitude to Task		Combining error probability from nodes 6.8 and 6.11
6.11	Workface Stress	Distraction	Combining error probability from nodes 6.9, 7.12
6.12	Task	Installation error	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error Probability	Combining error probability from nodes 5.9, 6.12
7	**Individual Factors (Active or Dormant)**		
7.6	Technical Knowledge and Skills	Task planning	Combining error probability from nodes 7.4, 7.5
7.12	Individual Traits	Error Probability	Combining error probability from nodes 7.7, 7.8, 7.11

11	**Error Probability Defences and Consequences**		
11.1	CAW Management	Error probability	Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145	Error Missed	
11.3	Consequences Pt 145	No Effect Error CF	
11.4	Release to Fly	Error Probability	Combining error probability from nodes 11.1, 11.5
11.5	Defence Pt M	Error Missed	
11.6	Consequences Pt M	No Effect Error CF	
11.7	Handling and Despatch	Error Probability	Combining error probability from nodes 3.26, 8.30, 9.12, 11.4, 11.8,
11.8	Defence H and D	Error Missed	
11.9	Consequence H and D	No Effect Error CF	
11.10	Defence Pre Take Off	Error Missed	
11.11	Take Off	Error Probability	Combining error probability from nodes 11.7, 11.10
11.12	Consequence Pre Take Off	No Effect Error CF	
11.13	Flight and Consequences	Flt Completed Error CF No Cost	
11.14	Combined Cost	Cost group 5	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14

Serial No	Report No	Aircraft	Date
4	X101/**/**/****	Type_A2 G-****	30 Mar 09

Inoperative cargo deck rollers.

On 29 Mar 08 a satellite station (*******) had reported problems encountered with inoperative rollers in the cargo deck of an aircraft. On 2 Apr 08 inspection and repair of the cargo deck rollers had been undertaken at the main base (*****) during which it was expected that the defectives rollers would have been replaced. On 3 Apr 08, Senior Line Maintenance Manger was following up the progress of the previously reported defect, when he had the opportunity of inspecting the state of rollers and reviewing the work done on the aircraft on 2 Apr 08, i.e. 2-sectors ago.

The job card reported that the rollers inspected and greased and several roller bearings were replaced where required.

However physical evidence offered quite a different story suggesting that the work had not been properly carried out. The task involved 210 bearings but only one engineer had placed his stamp for the work done even though 3-engineers were on duty during the shift. Part numbers of the bearings and components, claimed to have been replaced, had not been recorded on the job card, even though the local store records confirmed some items had been issued against this aircraft at the time. The task had logged 10.5 man-hours.

In view of the poor workmanship, the job card was reworked on 3 Apr 08 to a higher standard that needed the removal of bearing trays, disassembly, cleaning, inspection, greasing and reassembly of the bearings and trays. In the process the engineers found that grease injected during the previous maintenance operation on 2nd Apr 08 had not penetrated the bearing properly. 28 bearing assemblies at the entrance area of the cargo bay was not repairable; these were replaced. Six engineers were employed on rework that took 18-mon hours.

Quality audit who carried out the investigation had concluded that even though the first maintenance activity just met the task specification, it had not been effective in meeting the purpose. The second was a more thorough process that went beyond the task specification but met the intended purpose. The report recommended that the task requirement and relevant job card be reviewed and revised by Technical Services with the objective of the task achieving its intended purpose.

Comments: Subject bearings, being part of aircraft role equipment, offered no direct airworthiness implications, although one could surmise that if a heavy container went out of control due to failed bearings could cause structural damage to the cargo bay or injury to personnel in the vicinity. The direct effect of poor maintenance standard was inoperative rollers that could affect loading and unloading, and hence turn round times. Certainly it could affect the main operational role of this aircraft and of course, and if the problem is widespread, then it would affect company's line of revenue.

Although the SR did not dwell on it, evidence suggests that there is a need to review the documentation standards as well as workplace practices.

It was stated that the aircraft had flown 2-sectors following the first maintenance operation. In retrospect, it can be assumed that errors were present and therefore they were taken into account in the risk model as sectors flown with an error present but undetected.

4	X101/**/**/****	Type_A2 G-****	30 Mar 09
Error 4a – Four sectors flown 4a – 4d			
Index	**Node Name Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type A2	
1.3	Registration Number	Reg 6	
1.4	Aircraft Age	Over 25 to 30yr	
1.5	Number of Sectors Flown	****	
1.6	Number of Major Maintenance Cycles	*	
1.7	Aircraft	Error Probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error Probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	****	
1.15	Geographical Location & Time	Error Probability	Combining error probability from nodes 1.12-1.14
1.26	Operation V Capability	Error Probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
5	**Pt M AO Error Performance (Active or Dormant)**		
5.3	Pt M Sub Pt D Maintenance Standards	MA402 Maintenance Performance	
5.9	Pt M and Pt 145 Contract Interface	Quality control	
5.10	Pt M and Pt 145 Interface	Error Probability	Combining error probability from nodes 5.8 – 5.9
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.1	Pt 145 Organizational Performance	A50 Certification of maintenance	Combining error probability from nodes 5.10, 9.12
6.10	Attitude to Task	Others	Combining error probability from nodes 6.8 and 6.11
6.11	Workface Stress	Time constraint	Combining error probability from nodes 6.9, 7.12
6.12	Task	Poor maintenance practice	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error Probability	Combining error probability from nodes 5.9, 6.12
8	**QMS Organization and Performance**		
8.17	Pt 145 Activity Area	Line Stations	
8.20	Pt 145 Quality Audit Performance	Error Probability	Combining error probability from nodes 8.17 – 8.19

11	**Error Probability Defences and Consequences**		
11.1	CAW Management	Error probability	Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145	Error Detected	
11.3	Consequences Pt 145	No Effect Error CF	
11.4	Release to Fly	Error Probability	Combining error probability from nodes 11.1, 11.5
11.5	Defence Pt M	Error Detected	
11.6	Consequences Pt M	No Effect Error CF	
11.7	Handling and Despatch	Error Probability	Combining error probability from nodes 3.26, 8.30, 9.12, 11.4, 11.8,
11.8	Defence H and D	Error Detected	
11.9	Consequence H and D	No Effect Error CF	
11.10	Defence Pre Take Off	Error Detected	
11.11	Take Off	Error Probability	Combining error probability from nodes 11.7, 11.10
11.12	Consequence Pre Take Off	No Effect Error CF	
11.13	Flight and Consequences	Flt Completed Error CF No Cost	
11.14	Combined Cost	No Cost	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14
Error 4b-4c			
Index	**Node Name Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type A2	
1.3	Registration Number	Reg 6	
1.4	Aircraft Age	Over 25 to 30yr	
1.5	Number of Sectors Flown	****	
1.6	Number of Major Maintenance Cycles	*	
1.7	Aircraft	Error Probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error Probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	*****	
1.15	Geographical Location & Time	Error Probability	Combining error probability from nodes 1.12-1.14

1.26	Operation V Capability	Error Probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
5	**Pt M AO Error Performance (Active or Dormant)**		
5.3	Pt M Sub Pt D Maintenance Standards	MA402 Maintenance Performance	
5.9	Pt M and Pt 145 Contract Interface	Quality control	
5.10	Pt M and Pt 145 Interface	Error Probability	Combining error probability from nodes 5.8 – 5.9
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.1	Pt 145 Organizational Performance	A50 Certification of maintenance	Combining error probability from nodes 5.10, 9.12
6.10	Attitude to Task	Others	Combining error probability from nodes 6.8 and 6.11
6.11	Workface Stress	Time constraint	Combining error probability from nodes 6.9, 7.12
6.12	Task	Poor maintenance practice	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error Probability	Combining error probability from nodes 5.9, 6.12
8	**QMS Organization and Performance**		
8.17	Pt 145 Activity Area	Line Stations	
8.20	Pt 145 Quality Audit Performance	Error Probability	Combining error probability from nodes 8.17 – 8.19
11	**Error Probability Defences and Consequences**		
11.1	CAW Management	Error probability	Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145	Error Missed	
11.3	Consequences Pt 145	No Effect Error CF	
11.4	Release to Fly	Error Probability	Combining error probability from nodes 11.1, 11.5
11.5	Defence Pt M	Error Missed	
11.6	Consequences Pt M	No Effect Error CF	
11.7	Handling and Despatch	Error Probability	Combining error probability from nodes 3.26, 8.30, 9.12, 11.4, 11.8,
11.8	Defence H and D	Error Missed	
11.9	Consequence H and D	No Effect Error CF	
11.10	Defence Pre Take Off	Error Missed	
11.11	Take Off	Error Probability	Combining error probability from nodes 11.7, 11.10
11.12	Consequence Pre Take Off	No Effect Error CF	
11.13	Flight and Consequences	Flt Completed Error CF No Cost	

11.14	Combined Cost	No Cost	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14
Error 4d			
Index	**Node Name Secondary Level**	**Tertiary Level CF**	**Remarks**
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing	Type A2	
1.3	Registration Number	Reg 6	
1.4	Aircraft Age	Over 25 to 30yr	
1.5	Number of Sectors Flown	****	
1.6	Number of Major Maintenance Cycles	*	
1.7	Aircraft	Error Probability	Combines error probability from nodes 1.1-1.6
1.9	Operating Role	Cargo	
1.11	Nature of Operation	Error Probability	Combining error probability from nodes 1.8-1.10
1.12	Flight Origin	*****	
1.15	Geographical Location & Time	Error Probability	Combining error probability from nodes 1.12-1.14
1.26	Operation V Capability	Error Probability	Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25
5	**Pt M AO Error Performance (Active or Dormant)**		
5.3	Pt M Sub Pt D Maintenance Standards	MA402 Maintenance Performance	
5.9	Pt M and Pt 145 Contract Interface	Quality control	
5.10	Pt M and Pt 145 Interface	Error Probability	Combining error probability from nodes 5.8 – 5.9
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.1	Pt 145 Organizational Performance	A50 Certification of maintenance	Combining error probability from nodes 5.10, 9.12
6.10	Attitude to Task	Others	Combining error probability from nodes 6.8 and 6.11
6.11	Workface Stress	Time constraint	Combining error probability from nodes 6.9, 7.12
6.12	Task	Poor maintenance practice	Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance	Error Probability	Combining error probability from nodes 5.9, 6.12
8	**QMS Organization and Performance**		
8.17	Pt 145 Activity Area	Line Stations	
8.20	Pt 145 Quality Audit Performance	Error Probability	Combining error probability from nodes 8.17 – 8.19

11	**Error Probability Defences and Consequences**		
11.1	CAW Management	Error probability	Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145	Error Missed	
11.3	Consequences Pt 145	No Effect Error CF	
11.4	Release to Fly	Error Probability	Combining error probability from nodes 11.1, 11.5
11.5	Defence Pt M	Error Detected	
11.6	Consequences Pt M	Flt Delay Error Inv Rectified	
11.14	Combined Cost	Cost group 5	Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14

Serial No	Report No	Aircraft	Date
35	X124/**/**/****	Type_A2 G-****	21 Apr 09

Post C-Check acceptance checks. Flight crew oxygen system, low pressure side, leaking.

The post C-check acceptance test had been carried out at the receiving base where the accumulator pressure had been monitored, because the accumulator pressure had dropped to less than half the charged pressure.

Investigations had revealed that there was a leak from the low pressure side of the manifold to the captain's flexible pipe. The connection was re-seated, re-torqued and leak tested. Defect did not recur.

MEDA investigation failed to reveal a definite cause. However it was revealed that during C- Check at ******, insulation blanket replacement had been carried out, for which oxygen supply system had been disturbed and reinstalled later.

The certifying engineer for the task of oxygen system reinstallation had been interviewed, but had claimed that he could not remember working on it, and no one else had owned up to having done the work.

Causal factor was attributed to lack of stage checking records. These have been introduced since then as a preventive measure.

Comments: This is the second case (out of the 41 miscellaneous errors) where this specific Pt 145 MRO attributed an HF error to lack of stage checking, suggesting that its task management procedures are below acceptable standards. Hopefully stage checking records would alleviate future arising.

As to the individual engineer, it is bizarre that an engineer employed by a licensed Part 145 Approved Organization could disclaim responsibility for his signed up work on the grounds of absent mindedness. One implication is that someone else had fraudulently used his rubber stamp to certify a task that he had not performed or supervised. This would have more serious implications as it would undermine the integrity of engineers employed by that AO as well as the integrity of AO itself as a reliable organization trusted to undertake aircraft work.

Serial No	Report No	Aircraft	Date
37	X173/**/**/****	Type_A2 G-****	30 May 09

Erratic tech log entry on the ADD log.

Despite the failure of a stand-by power system check noted during A-Check, the Tech Log line was cleared on the ADD Deferred Defect log, enabling the aircraft to fly, whereas in reality, standby power was a No-Go item. The error was discovered in time by another engineer, before the next flight, placing the aircraft AOG for further investigation.

The aircraft was released to service the following day after replacing one of the relays and checking the serviceability state of the aircraft. The individual was interviewed and placed on, “return to continuation training”. Continuation Training program was amended to include this new item.

Comments: A straightforward case of individual error due to limited experience and most likely limited knowledge on the stand-by power system.

Serial No	Report No	Aircraft	Date
39	X206/**/**/****	TYPE_A2 G-****	24 Jun 09

RH Fuel Shut Off Valve (SOV) connector Pin 6 had no 28V DC power.

During embodiment of a Service Bulletin concurrently with a C-Check at contracted MRO (******) it was found that the right-hand fuel shut off valve (SOV) connector Pin 6 had no 28 V DC power. Investigation revealed that there was a break in the power supply cable in the RH engine strut, where there was sign of a "splice assembly". On opening up the assembly, it was found that the cable was severed inside and not properly spliced.

There has been no previous repair of this line by the current operator, and therefore it was assumed that the broken cable was the result of a previous repair done whilst the aircraft was in the custody of the previous operator.

Comments: This is a good example of a dormant human error that could have lead to serious consequences if and when adverse conditions lined up. On transfer of aircraft to subsequent owners, not all technical documents get transferred, and therefore it is up to the new owner (or their surveyors) to demand a comprehensive pack of historical records, and to undertake necessary reviews. Naturally, in commercial situations, it might not be practical or even feasible to insist on the full historical document suite, thus the new owner accepting a degree of risk with second hand aircraft. It is highly likely that older aircraft that had undergone maintenance carry dormant errors; greater the amount of maintenance, greater the amount of human errors they might be carrying. To anticipate this type of dormant hazard, the CAW Risk Model tries to build up a reference baseline by requesting information on the age of the aircraft, usage and the number of major maintenance cycles that it had undergone.

Serial No	Report No	Aircraft	Date
40	X222/**/**/****	TYPE_A2 G-****	3 Jul 09

Forgotten APU Battery Charger CB caused batteries to overheat and spill chemicals

This error, committed at one satellite station (*******) was discovered two-days later at another satellite station (probably ***** in *******) where it was rectified,

An engineer, who was called out to clear an APU Battery Charger status error-message, could not clear the error/ defect because a spare was not available. However being a non-safety critical item, he cleared the tech log entry with an ADD thus allowing the aircraft to depart, but forgot to remove the circuit breakers to deactivate the charger.

The charger continued to charge, overheating the battery and spilling fluids, which was discovered 2-days later by another engineer based at another satellite station.

MEDA investigation was carried out by ****** who employed the first engineer at the station where the work was undertaken. The engineer admitted failing to remove CB. He had overlooked the need to complete the maintenance action, having simply assumed that the APU Battery Charger was not an airworthiness item. Focussing on getting the aircraft airborne as it had already been delayed, he had cleared the error message with an ADD, and immediately moved on to do another task, to which he had already been assigned by his controller.

Investigation revealed that the engineer had been under abnormal pressure, having pulled out from another defect rectification job to attend to the APU Battery Charger and then immediately afterwards to attend to a 3rd aircraft that was waiting for his attention.

The engineer was highly experienced (26-years service) with many type ratings. He has had a spotless record in the employer's books. That, together with his prompt coming forward to acknowledge his error and his explanation of the circumstances, had been helpful to draw a conclusion that this was a case of distraction due to unusual pressures put on the engineer.

Comments: An example where manpower is below adequate to meet peak demands. Although everyone has the good intention of serving management objectives, in this case it has been done at the expense of safety. The consequences could have been worse. HF teaching call for the engineer to inform control that he was getting stressed, but it was equally likely that the engineer was either thinking that he was coping under stress or, if he was not coping, then he did not want to raise an issue in case it was taken against him.

The model included information on the sector where the error was first introduced, the sector that demonstrated the presence of an error, as well as the sectors flown during the 2-days that the aircraft was carrying the error.

Serial No	Report No	Aircraft	Date
43	X246/**/**/****	Type_A2 G-****	2 Aug 09

Circuit breakers left, "pulled," post maintenance.

On crewing in, the flight crew found Main and Auxiliary Left & Right Pitot Heater circuit CB's pulled; Left & Right AOA CBs pulled; Temp Probe CBs pulled; Battery Switch was ON and position lights OFF. There was no reference to the above in the tech log, nor placards placed on the CB panel.

A mechanic had worked on a side window heating problem. On interview the mechanic had claimed that he did not need to pull these CBs and had confirmed that he had followed the rules and procedures iaw the FIM (Flight Information Manual). He had also said that at the time he finished his work, he did not notice any pulled CBs at all.

A continuation training letter had been raised to remind engineers on the correct procedures and disciplines to be adhered to when pulling CBs.

Comments: The investigation had not been taken to its natural conclusion and seemed to have been truncated after the mechanics statement, presumably on the ground that the error had been found before it caused any damage and that it was not cost effective to follow through. The possibilities were:

1. Someone must have pulled them out erroneously and then got distracted, or
2. Someone deliberately pulled them to do another task and then got forgotten during trying to finish the job fast
3. Left forgotten by flight crew from the previous sector
4. Pulled by a mischief maker with intent.

It was noted that other ground crew who went to assist prepare aircraft, ahead of the flight crew did not notice pulled CBs, because the pulled CBs were concealed by other furniture in cockpit and there were no tell-tale placards placed on pulled CBs.

If tech log did not reflect any work on the Pitot System, or AOA, or anything associated with it since the end of the last sector, then suspicion falls on the mechanic who worked on window heating, unless flight crew had pulled them out for some other reason.

It was noted during this survey of errors, that on the same date, a CB panel had been robbed from another aircraft by another engineer without strictly adhering to correct procedures. In that situation, there had been verbal agreement between the parties involved, but timely documentation had not taken place. Investigator had not mentioned this fact in the investigation report to establish if there had been any connection between the 2 events or, if not, to separate them as independent events. See Serial No: 44.

Limitation of getting to the bottom of the truth could be due to local constraints such as cost-effectiveness or impact on labour relations. The investigator's recommendation to improve Continuation Training might be the optimum solution, even though it might not have addressed the real causal factor.

Serial No	Report No	Aircraft	Date
44	X249/**/**/****	Type_A2 G-****	2 Aug 09

CB robbed without formal approval and following improper documentation procedure.

A CB assembly had been robbed from G-**** undergoing A-check, to service another aircraft OO-*** required for flying. The robbing was verbally approved by *** MOC Duty Controller but he failed to follow up with an approval number and paperwork that was promised to be dispatched.

The Duty Line Manager at the satellite station (*******) verbally authorized the engineer to carry out the robbing, assuming that paperwork had arrived and that they were in engineer's hands.

In any event, the engineer who carried out the work failed to make proper entries in G-**** Tech Log. Subsequent to the completion of robbing, ****** he raised the form for robbing, filled in the known information and faxed it to **** MOC.

Comments: The situation described is typical for a team working together to achieve an objective with good intention but in the process the parties involved had infringed the rules by trying to short circuit the correct procedure. Verbal agreements are usually made between the parties to get a job done on the promise that paperwork would be followed up; it is a typical industrial situation, but in this case the promise had not been followed up in a timely fashion. Senior managers had made important decisions based on assumptions and without asking the right question. Ironically, the team had broken the very same rules that was intended to prevent this type of error occurring. The situation was compounded by the engineer failing to finalise the Tech Log entries correctly.

Lack of comprehension of the procedures and miscommunication had been identified as the root causes. These are both organizational and individual errors.

Action taken to introduce relevant subject and procedures to continuation training program would hopefully alleviate future occurrences, but it is a topic worth repeating.

Unavailability of parts is a further contributory causal factor, and this should reflect on funding and resourcing at corporate level; it is their responsibility to ensure and fund the activities of Heads of Engineering and Logistic, so that they are effective in getting spares assets to where they are urgently required.

Serial No	Report No	Aircraft	Date
47	X258/**/**/****	Type_A2 G-****	10 Aug 09

APU oil empty due to incorrectly installed filler cap.

Flight crew on completion of ****-**** sector had reported APU oil empty despite last replenished on the 10 Aug 09. On the 10 Aug 09, at ******, the aircraft APU had been replenished by a mechanic and fastened the filler cap. Another mechanic has checked the oil level, and ascertained that it was full, had checked the security of the filler cap and signed for the work. The person who signed for the task was called to account for the error but could not explain how the error could have happened. He was reminded that a Cat-A mechanic could only sign for his own work and not others.

Comments: Two errors had been committed, one procedural error on signing up for the work done, and the other faulty installation of the filler cap. The second error has been unaccounted for except, one can surmise that it was cross-threaded and was not properly sealing the filler neck. Investigation incomplete in so far as follow up actions to prevent recurrence.

Serial No	Report No	Aircraft	Date
48	X260/**/**/****	Type_A2 G-****	24 Aug 09

Incorrect Decal markings at fuel drip-stick locations on both wings

An aircraft had been returned from post-Scribe line inspection, with the "Fuel Drip-Stick" locations' decal markings placed in reverse order, i.e. 1-7 (inboard to outboard locations) instead of the original No: 6-1 (inboard to outboard) with No: 7 furthest outboard.

By way of a solution, except the positions No 2 left wing and No: 6 both wings, decals were reverted to the original positions. The exceptions were entered on White ADD, pending availability of spare decals.

The aircraft manufacturer, on seeking their advice, had suggested that decals could be positioned either way, and a ruling has yet to be issued by the manufacturer.

Comments: This report has been posted as a maintenance error. It appears to be a production issue, because according the manufacturer there are 2-correct versions for decal positions. Await further advice from the manufacturer.

Serial No	Report No	Aircraft	Date
51	X278/**/**/****	Type_A2 G-****	26 Aug 09
Gear pin stowage missing.			
Flight crew noted that undercarriage lock pins were not in their usual stowage on the rear cockpit wall, and that the stowage box was missing, but there was no Tech Log entry to indicate the status. Pins were found in the vestibule cupboard adjacent flight crew location. Since then engineers had raised a WADD and subsequently replaced the stowage and cleared the WADD.			
Comments: The error was in documentation and failure to report the status of the aircraft through Tech Log entry and the raising of the WADD to clear it temporarily			

Serial No	Report No	Aircraft	Date
55	X285/**/**/****	Type_A2 G-****	28 Aug 09

Remove before Flight Tape left onboard and found during post-flight walk round.

During the post-flight walk round after a sector ****** to *******, the captain noted a "Remove Before Flight" tape hanging underneath the RH wing of the aircraft.

An engineer working in a night shift and diagnosing a hydraulic leak, had left a warning flag for the benefit of his colleagues to indicate the likely source of leak. He had left a written note about the warning flag on the Supervisor's Diary. Unfortunately the day-shift who provided continuity with the diagnosis had started to work from another location of the aircraft, from where the tape was not visible.

Meanwhile an entirely separate task on the same aircraft to diagnose "RH wing low" defect had necessitated the lowering of the flap and rigging the aileron flush. In this process, the tape got put aside; at the end of the second task the flap was left at the retracted position, trapping the now folded and stowed away tape out of view.

Since neither a separate task card nor a Tech Log entry for the removal of the tape had been raised, the hidden tape got unaccounted for, until it got unfolded and became visible when the flap was extended during the subsequent flight. The following human errors had occurred:

- Engineer No: 1 failed to raise a supplementary card, or an entry in the Tech Log.
- The night shift Supervisor who put the information in the Handover Diary to tell his engineer to raise a supplementary card or tech log entry, or to raise them himself. But he failed to act on it. This is an error at the defence level.
- The day shift Supervisor who took over the diary failed to act on the diary entry regarding the tape. He continued to work his normal routine, oblivious to the danger.
- Engineer No: 2 of the day shift did not trace back and clear the work areas, concentrating his effort only in the area that he worked. It might be possible that he did not see the presence of the tape, because by then it was already been stowed inside the wing, to provide a clear space for the extended flap.

Comments: This is yet another error committed due to lack of discipline in raising a supplementary job card or a Tech Log entry to cover new maintenance tasks or where they are not part of the normal task schedule.

Serial No	Report No	Aircraft	Date
50	X273/**/**/***	Type_A2 G-****	31 Aug 09

MEL not followed, initially, to clear status message ("R ELEV PCU").

This relates to an attempt by third party contracted engineers at a satellite station to clear an EICAS message on the hydraulic system. Ground engineers worked to their local MEL which was different from the operator's MEL and put the aircraft unserviceable. Eventually the problem was resolved by the operator's engineers that enabled the flight crew to have enough confidence to fly the aircraft back to the main base where the defect was rectified.

Eventually the hydraulic system's faulty components were replaced, and the system tested and proved to work satisfactorily. Since then the aircraft had flown 76 or more sectors, satisfactorily.

Comments: The key issue involved is the disparity between the two MELs: one used by operator and the other used by the third party contractor. It was the responsibility of the Part M organization undertaking contracting-out to ensure that standards and specifications are defined.

Another related issue is the failure of Quality Audit system to pick up this disparity.

Neither the MEDA report nor SR fails to state what action was proposed to prevent a recurrence. It might be necessary for the operator's quality management system should review the MEL requirements and agree on the MEL to be used against operator's aircraft.

Serial No	Report No	Aircraft	Date
53	X280/**/**/****	Type_A2 G-****	31 Aug 09

R1 door opened without deactivating the power assist

Five minutes before takeoff, the captain called an engineer to check out an EICAS message on speed brakes. During functional test, the Front right (R1) Door was opened for the engineer to physically observe the spoiler panels operating. During door opening, the Power Assist Bottle was activated accidentally.

The engineer stated during the interview that he might not have moved the selector lever correctly, because under time-pressures consistent with the high morning work load, he was in a hurry.

SR does not discuss recovery action or if any disciplinary action was taken.

Comments: This is an example of engineers working under acute time-pressures making mistakes, as their alertness and mindfulness for the job at hand is lacking. Whilst the engineer is physically on the current job, his mind seemed to be working on the jobs on his list and how he is going to manage his time to fit all the tasks, or even mentally working on the next job to do.

There was no investigation into the reasons why this engineer as over stressed at work, why he was tasked with so much work, or if there was shortfall of staff as well as line managers. Was the organization at fault to expect too much from their engineers? Could the limited trade cover provided cope with peak demands, and if not what alleviation is allowed to engineers working under pressure to ensure sufficient safety level is achieved and maintained? Are engineers allowed to state their opinion on the workload without getting marked-down for stating their concerns? These are some of the management challenges that managers must face constructively so that they could be resolved without detriment to flight safety.

If organizations do not have standard times for tasks, then this is a good example to demonstrate that there should be standard timescales for work stints, and manpower should be provided to meet peak demands. If standard times are available, then it is possible to rate the jobs, and manning accordingly or if not set up other defences.

Serial No	Report No	Aircraft	Date
46	X256/**/**/****	Type_A2 G-****	9 Aug 09

No 2 Engine thrust reverser sensor loose and out of adjustment.

An aircraft was due to be flown back to the base from a satellite station to have its defective No: 2 engine thrust reversers (TR) repaired. During the previous night an engineer at the satellite station had worked on the TR, leaving the task to be completed by the engineer working the day-shift.

Assuming that all the work up to that point had been satisfactorily completed, the LAE, working the day-shift, had then signed off the work done on the thrust reverser, without first having properly checked if the previous stint of work had been satisfactorily completed.

Because of this omission to check, he was not aware of the true state of the TR. In consequence, his documentation and certification on the Tech Log was faulty, and moreover he failed to notify the flight crew about a problem relating to TR stowage.

The aircraft had been released to service in this state for the ferry flight to base. The outcome was that the flight crew using the thrust reverser after landing was getting intermittent warning messages on the EICAS and also while attempting to stow the TR..

During the investigation that followed, it was found that the thrust reverser had not been correctly rigged, that it could not be properly stowed, and that the (stowage position) sensor was loose and out of adjustment. This was the reason for intermittent warnings. In fact, because of incorrect rigging, the TR could not be even manually stowed and locked.

Investigation had also revealed that the engineer involved had violated a number of procedural steps, in that he was culpable for:

- The failure to correctly assess the worksheets and the status of the reverser being worked.
- Entering the defect incorrectly into the sector record page and under incorrect deferred defect category, i.e. “White” ADD, instead of a “Pink” ADD. The Pink ADD warns of operational limitations, as it was in this case.

Disciplinary action against the engineer was being considered. The MEDA findings were to be disseminated to the organization’s workforce through Continuation Training program.

Comments: No further comments.

Serial No	Report No	Aircraft	Date
11	X390/**/**/****	Type_A1 G-****	11 Sep 09

3-Day over run of fuel sump draining task

An aircraft that has undergone base servicing at an MRO (*******) was about to be handed over to the operator on the due date, when the MRO management suddenly declared an outstanding missed task. There had been 6 previous pre-handover conferences about outstanding tasks, but this task had not been flagged up. It appeared that during the course of the base servicing there had been an omission in the management of and accountability for the tasks set on the MRO due to human error. This Safety Report had been raised to document this human error.

Comments: There was no clear explanation of the background to this incident or to causal factors for the omission to account for the misplaced/ untracked task. On the face of the information presented, there appears to be a contractual issue involved between the operator and the MRO. Clearly terms of the interface contract, and the way task specification and standards must be audited by operator's quality department as per EASA regulations.

Serial No	Report No	Aircraft	Date
1	X299/**/**/****	Type_A1 G-****	15 Sep 09

During walk round, No.12 slat leading edge found not faired with winglet and top wing panel not flush.

Two separate aircraft defects attributed to human errors had been reported.

1. RH Leading edge slat wedge interfering with No: 12 slat.
2. R/H outboard aileron contacting the winglet, upper seal-retainer during aileron full up position.

The second defect was found whilst investigating the first error. This aircraft had undergone conversion in the US, by an approved organization contracted by the original equipment manufacturer.

The root cause of the R/H leading edge slat wedge interference with the No.12 slat had been attributed to poor installation by individuals employed by the approved organization and subsequent failing by quality checkers.

The root cause of the R/H winglet aileron clearance problem can be attributed to either errors or lack of clarity in technical documents/instructions.

Similar problems had been encountered during the conversion of the operator's two other aircraft of this type. As a result of this error, another technical instruction has been issued to check the gap between the bulb seal retainer and the upper outboard forward edge of the outboard aileron on all similar aircraft modified by the winglet installation STC.
As part of a long term solution, the design specification of the winglet STC installation was being reviewed by the Design Authority in conjunction with FAA, EASA and UK CAA.

Comments: These errors were spotted at the flight line of the operator only after a new aircraft had been delivered. The primary error was committed during the embodiment of the winglet installation modification where the fouling of the structure should have been spotted and reported.
Causal chain investigation would have pointed to errors in Part 21 AO's internal quality control system, errors in the detail design of the winglet installation and its clearance by airworthiness authorities as contributory factors; these areas were not open to MEDA investigator.

It is not uncommon for some employees of airworthiness authorities to claim that their role is only procedural and is driven by written information provided by the designer.

Serial No	Report No	Aircraft	Date
57	X300/**/**/****	Type_A1 G- ****	15 Sep 09

Engineer slipped, sprained ankle and damaged skin of the outboard aileron.

Whilst preparing the aircraft for a RH wing outboard aileron rigging check during morning of 15 Sep 09, the engineer slipped on condensation that had formed on the safety raiser platform. As a consequence he accidentally dropped the rigging bar on the aileron puncturing the upper skin made of composite structural material.

The puncture was initially repaired with aluminium-foil tape. Two White-ADDs were placed in the Tech Log, one to inspect the tape at every 50 cycles and the other to repair the puncture within 300 cycles. On the 17th Sep 09, the aileron was given a permanent repair and the 2 ADD entries were cleared.

The individual suffered a sprained ankle. An accident/personal injury report was raised, but he did not require any further medical treatment nor wanted time off to recover.

Comments: This is mainly a Health and Safety issue that lead to a human factors related damage to an expensive aircraft structural component.

It does raise the question of the type and suitability of safety raiser, their husbandry and preparation before use. A man has been injured and an aircraft damage. If condensation is a causal factor, then foot grip on safety raiser platforms and walkways should be improved to prevent recurrence of similar events or even death by falling off a platform or a wing surface. Individuals and management have a duty of care and part of that would be using the right type of clothing and footwear, as well as good husbandry and preparation of equipment before use.

Serial No	Report No	Aircraft	Date
5	X317/**/**/****	Type_A2 G-****	24 Sep 09

Aircraft was felt "light" on take-off rotation. Incorrect assembly of elevator feel unit.

Following a captain's report that the aircraft was felt "light" on rotation during take-off and that nose oleo appeared higher than normal, a nose oleo leg shock strut servicing was initially carried out. The aircraft flew 3 more sectors without complaint from flight crew and on the 4th sector the abnormal feel was again reported. Detailed investigation of the elevator feel and centring unit followed, when a "cracked" upper forward spring roller bearing in the elevator neutral shift support bracket was found. In addition, incorrect assembly of 2 springs on the elevator feel and centring assembly and of adjuster shims were also found.

Incorrect orientation of springs had been attributed to ambiguity of AMM drawings. Once the damaged components were replaced, mis-assembly was put right, and system functionally tested, the aircraft handled as expected with no further complaints from flight crew.

Maintenance record had confirmed that between Nov 04 and Dec 06, some of the subject components had been either defect investigated, serviced or replaced 3-times. The roller bearings were also subjected to routine inspection and, repair as required, at every 2C-Check by MRO.

It was not known exactly when or where mis-assembly had taken place. However the aircraft manufacturer, OEM, had reported that the wrong orientation of the spring had no effect on the feel unless the spring was twisted. Nevertheless, OEM had agreed to amend drawings to remove any ambiguity.

Additionally, as an MOR had been raised and closed with a recommendation to amend the AMM and to review the need for bearing replacement during C-Check, when it is susceptible to human error,

Comments: As the origin of the defect was unknown this would have to be categorized as a dormant error. However it might be prudent to check when the last C-Check was completed before 24 Sep 09, because the "light" feel was a new report in September. There could have been a C-Check done after Dec 06, the last time the elevator computer was replaced, or 5 Nov 06 when Line repair was done on the elevator feel and centring unit.

Serial No	Report No	Aircraft	Date
59	X326/**/**/****	Type_A2 G-****	30 Sep 09

Aircraft arrived with reported Oil Smell In Cabin on both engines.

On 6th Oct 09, following reported Oil Smell in Cabin (OSIC), engineers at the base station, investigating the source of an oil leak in accordance with AMM (standard procedure) had to remove the engine spinner cap to see if there were signs of oil stains.

Although no oil was found, they found damage and distortion to the spinner and spinner cap locating area, signs of them being forced into position by an external force. The damaged items (front and aft sections of the spinner and the anti-icing duct) were replaced at a cost of USD 80,682.

Prior to this date, there had been several other attempts to locate the source of OSIC. Following up a previous report from one satellite station, line engineers at another station had already removed and reinstalled the spinner cap on 2 Oct 09 as part of their investigation into LH AC pack. Again, on 4th Oct 09, RH AC pack was investigated by the first satellite station, when the spinner was removed and reinstalled. Both these investigations proved negative.

It was during this third attempt at the main base when damage to the spinner was discovered and reported.

This damage was referred to the first satellite station where the previous defect investigation was conducted. Whilst engineers there acknowledged that damage was possible, they did not accept liability for it, pointing out that this sort of investigation had been repeated several times before, and that there was no way of identifying exactly when or where the damage had occurred.

Further investigations had revealed that the design of the anti icing duct was not conducive to ease of assembly in situ. It has been mentioned that one had to let go of the tube before offering up the spinner cap, when the former drops and gets out of alignment. This could be the main reason that fouling occurs, and out of alignment causing many problems including forceful application of percussion that causes distortion. Clearly this aspects should be investigated as part of finding a more lasting solution

In addition to the completion of repair to the damaged spinner, retraining of personnel has been introduced. A proposal to amend the AMM has been submitted as well as the opening up of further discussion with the aircraft manufacturer to determine a way of mitigating such circumstances.

Comments: In view of the difficulties experienced in re-assembling the spinner, one could presume that the damage was unintentional. Whereas this configuration might be more acceptable for a vertical position found in a depot type assembly line, in the horizontal position found at an operational base, locating the oil tube could be a real problem.

Considering the cost and frequency of replacing damage prone components, the operator should consider possible design changes as follows:

1. To provide an endoprobe-type inspection hole to inspect the presence of oil in the spinner assembly.

2. To provide a means of stabilizing the anti-ice duct in a horizontal position, this may be like a keyway and spline, so that it would not drop when the spinner cap is being offered up.

Serial No	Report No	Aircraft	Date
6	X348/**/**/****	Type_A2 G-****	6 Oct 09

Components robbed from an uninstalled engine without following correct documentation procedures.

Three items were removed from an uninstalled engine to repair an installed engine on an in-use aircraft. At a later date when the required spares arrived, engineers found that there were no open servicing documents identifying where they were to be fitted. Subsequent investigations revealed that a number of errors had been committed at work face, coordination, higher level of management, as well as other shortfalls in the quality management system.

Documentation at the point of operation was faulty.

- Lead engineer who removed components did not check the rules and documentation procedures for "uninstalled to installed engine" component robbing. He had assumed that the procedure was same as "installed engine to installed engine" robbing, and acted accordingly, thereby omitted raising a Non Routine Work Card.
- His helper, another licensed engineer acted as a mechanic removing the components without taking responsibility for paperwork, which he assumed was the domain of the lead engineer. He also failed to read the relevant procedures, and was content to provide labour only.
- In the absence of a Non Routine Work card, no instructions had been left concerning the repair of the "robbed" uninstalled engine when spares arrived.

Authorization process for robbing and documentation was faulty.

- Robbing approval could be given only by Tech Director (TD) who should sign the authorization form held by Maintenance Operations Centre (MOC), but in this case a Deputy Line Maintenance Manager (DLMM) provided verbal authorization to MOC who in turn signed the form on behalf of TD. This variation was contrary to authorized procedure.
- DLMM had claimed he spoke to TD and got his approval, but TD could not recall the conversation.
- TD had been under the impression that the rules of authorizations had been relaxed, but had not followed through to align intended policy change. In fact TD was vague on the policy and reality.

Quality Audit System that was in place to oversee if the procedures were proper and effective missed this particular process

- Finally, the quality audit system had failed to provide sufficient oversight in this area, thus missing to spot the prevailing abnormalities and correct them.

Overall, there has been a system failure: i.e. the defence mechanism that had been put in position to oversee and prevent the occurrence of error, had itself failed due to organizational or individual errors, thereby negating the defences. Although in this particular case the risk was categorized by the organization as "moderate" failure of the system was more serious because under a different set of circumstances that could lead to a catastrophic failure.

The following actions have been recommended to prevent a recurrence:

- Publish a revised policy and procedures.
- Educate the work force about the changes by amending the Continuation Training program
- QMS were to improve the Quality Audit requirements and processes.

Comments: This relates to an improper robbing procedure followed when robbing from an uninstalled engine to service an operational aircraft. Human error occurred at the workface relating to correct documentation, and at senior manager and coordinator levels that authorised and recorded the authorizations, and at QMS level where there ought to have been an adequate oversight of the robbing procedures.

In this case all 3 tiers failed, indicating a system failure where not only the error at work face got hidden but also the defence mechanisms that was supposed to detect the error and provide the defence mechanism. This is a good example of total system failure.

Fortunately the error was detected in time, and no serious consequences. Although the operational aircraft was not at risk, state of airworthiness of the uninstalled (a high-value asset) could have been left in doubt.

Serial No	Report No	Aircraft	Date
9	X335/**/**/****	Type_A2 G-****	6 Oct 09

Un-demanded operation of the left centre tank override pump.

Prior to the start of engines for ground running, fuel pumps were switched ON in an aircraft that was on a C-Check. Then it was noticed that the left centre tank override pump was operating voluntarily. This pump should only operate if the fuelling door is open or if the left engine is running, but in this case, the fuel door was closed and the engine had not yet started.

Investigations followed and the defect was traced to an electrical cable that has been capped and stowed incorrectly. The defect was rectified, after which the pump operated as expected.

The engineer reported that similar cases had been experienced by this MRO previously on two of the operator's aircraft. Further investigations confirmed that the two aircraft no longer had the wiring errors. But there were no records of rectification suggesting that they had not been formally reported, nor formally rectified. All the people and supervisors interviewed reported no knowledge of the past events, if there were any.

Fleet wide inspection of the operator's remaining aircraft revealed that 13 other aircraft had dormant wiring faults, although they were not identical to the first one that triggered off this investigation. All defective wiring was rectified before the next flight of the affected aircraft.

Comments: The report failed to identify the circumstances of the onset of error, when and where they that might have had occurred or the causal factors. It might be interesting to determine if all these 13 aircraft had recently undergone C-Check servicing at the same MRO; this had not been done.

One person volunteered information of the previous occurrences in good faith, but others denied any knowledge of it. MEDA investigation had been completed at the MRO itself but it had been inconclusive as to the root causes. The 13 aircraft have been separately identified in the spreadsheet.

Serial No	Report No	Aircraft	Date
60	333/**/**/****	Type_A2 G-****	6 Oct 09

Tech Log Open Defect.

This SR had been raised by a captain signing up for the pre-flight prior to flying a sector between 2 satellite stations (***** to ***** sector).

On the 6th Oct 09, a captain flying the ***** to **** sector had entered a defect on the main cargo door indication on the white page of the Tech Log against which two Pink ADDS 38/09 and 39/09 had been raised. The Tech Log entry had not been raised iaw the Ops Manual Part A 8.1.11.1.3.that applied to Flight Crew; he should have entered such defects in SRP, i.e. Sector Record Pages. He had signed the entry in the Tech Log but not in the Pink ADD, where he was allowed to sign as per Ops Manual.

On 6th Oct 09, ground engineers at **** tested the cargo door sensor several times, and as there were no unsatisfactory indications, PADD 39/09 was cleared leaving 38/09 open for further diagnosis.

Six sectors later, a captain operating **** to **** sector had noted the open PADD and reported the matter; this was the subject of this SR.

On 8th October a flight crew reported that they had EICAS messages about the door 3 times out of the previous 8 sectors flown.

On the 10th Oct 09, at **** engineers lubricated and exercised the main cargo door four interlock switch plungers. Two sectors later, as there had been no further error messages on EICAS, PADD 38/09 was cleared.

Furthermore on the 10th Oct 09, because of the history of defects on this door, base station engineers checked the wiring for the interlocking switch, but no faults found. The plungers were checked to see if any of them were on unlock position, with negative result. The plunger adjustments and tolerant were checked. After an operational check that was satisfactory, the aircraft was returned to service.

Comments: The issue here was a procedural error made by a flight crew member. The defect concerned was under investigation, and because of its intermittent nature, the relevant PADD had been left open. Defect in the main cargo door, indication system, was due to wear and tear. That is a reliability issue and not maintenance error.

Serial No	Report No	Aircraft	Date
62	X377/**/**/****	Type_B1 OO-***	24 Sep 09

Nose heavy at take off due rigging incorrect.

Flight crew had reported that the aircraft was nose heavy on previous take off and needed unusually long take off run. He was suspicious of the cargo loading but on checking this was found to be the not the cause. Fuel loading and instrumentation was also suspect and engineers were asked to look into contents gauges and dip stick figures or correlation, as well as the state of the stabilator trim positions.

However on walk round engineers (at *******) noted that the external markings of the Horizontal Stabilizer (THS) that can be trimmed were showing 1-unit nose down. On checking the cockpit stab trim wheel, it was indicating Zero (0) trim, which was a conflict. Engineers further found that the trim wheel did not travel full range in either direction.

This led to engineers undertaking a stab-trim rigging procedure iaw AMM. When the trim was set to X dimension, the cockpit trim control was -1.4 degree nose down, and when -0.3 was added to this the figure was -1.7 degree nose down which was clearly an error in the system. Therefore adjustments were made iaw AMM, and after further independent checks the aircraft was returned to service.

As the aircraft had been previously worked on by ****'s 3rd party contractor, and had Belgian Registration OO markings, further investigation was passed on to ******.

At the time of documenting, ***** had not responded, although 4 months had passed. Therefore the operator had decided to close this SR.

Comments: This is human error by those who undertook previous stab-trim control maintenance; clearly an error has been made during rigging check.

Serial No	Report No	Aircraft	Date
61	X371/**/**/****	Type_A2 G-****	27 Oct 09

MEL incorrect in identifying CBs to be pulled in case of Cargo Aft defect message.

Flight crew reported an error message relating to Cargo Aft Fan. Engineers tried to pull CBs as per MEL data, but found that only 2 MEL specified actually exist on the panel. AMM confirmed this, and so the engineer acted iaw AMM and released the aircraft as he had no more ground time (as the aircraft was to depart). The related PADD entry was left unclear.

On arrival at *******, the flight crew reported that he had no further messages during flight. Engineers at ******** reset the CBs, tested the cargo aft fan and heater satisfactorily and cleared the Pink ADD.

Further investigation by Tech Manager confirmed that the relevant part of the MEL, which was originally written for passenger aircraft, was incorrect for cargo aircraft. Consequently, a “pink-sheet” alert has been sent out to air and ground crews. MEL would be amended at the next cycle (C-Check?) in March 2010.

Comments: This is a maintenance/aircrew data error attributable to Part 21 AO Product Support (continuing airworthiness maintenance information for variants, vide Part 21 A.120) as well as Part M Sub Part D, 401, Maintenance Data.

Serial No	Report No	Aircraft	Date
7	X376/**/**/****	Type_B1. Reg No: NA	31 Oct 09

Aircraft released to fly with 2 worn tyres and brake-unit worn close to limit.

Post flight inspection of an aircraft arrived from **** to ***** revealed that the treads of No: 2 and No: 7 main wheels covers were worn all round the circumference, and at places the canvas was exposed. The aircraft had the weekly inspection completed at *****. ***** did not have spare covers, and having discussed the situation with MOC at *****, the aircraft was cleared for 2 more sectors and allowed to fly to *******. Wheels were sent from ***** to *******, where the wheels were replaced.

Safety report had yet to be completed, and was anticipating a report on the circumstances leading to the release of the aircraft from *****.

Comments: In this instance, there had been no adverse consequences such as runway excursion, tyre burst, damage to wheels or undercarriage struts, or wheel brake fire during landing. This may be more due to luck and design safety features, rather than to subtle maintenance practices.

It would appear that the 2-wheels were in different bogies. Most likely the other wheels were available and serviceable to carry the load. Engineers at ***** might have been relying on the fact that the aircraft was lightly loaded and that the load could be spread onto other wheels. However it is not clear if the aircraft would have passed a regulatory compliance test or an internal quality audit check.

Serial No	Report No	Aircraft	Date
2	X386/**/**/****	Type_A2 G-****	2 Nov 09

Service Check overdue by 12 days 20.3 hr.

Planning and scheduling support for this operator's aircraft is usually provided by ***** in ******** operating under the name *****.

On Monday 2nd Nov 2009 the ****** Planning Department noticed that the service check on this aircraft -**** was overdue by 12 days and 20.3 flight hours. At that time the aircraft was at a satellite station (*****). The aircraft was immediately grounded and a service check carried out. There were no findings.

Investigation revealed that the service check was last performed on 9 Sep 09 during C-Check at an MRO. TRAX was updated at the time and the next due date was correctly recorded as 21 Oct 09, provided the aircraft was released to service immediately. However, in this instance, there was delay from releasing the aircraft as it was undergoing C-Check. That means the actual date for implementing the C-Check would have to be adjusted and monitored manually, because during the C-Check the aircraft was not flying and the routine average daily utilization rate did not apply. The oversight in monitoring the due date was due to this manual estimation, which had gone wrong due to human error

Furthermore, an independent study had indicated that the actual daily utilization figures applicable to Service Checks were erratic, because the actual utilization figures were higher than the estimates. The TRAX system used for estimating due dates use these utilization figures. Because the system was prone to errors, the TRAX estimates have been increased to reflect more realistic values.

Comments: This report highlights a typical "Organizational Level" error. In this case the error was realized in good time and prompt recovery action was taken. However the issue raises some additional questions: Was it possible for the system to have made similar errors on other aircraft that had gone C-Checks before?

Serial No	Report No	Aircraft	Date
8	X380/**/**/****	Type_A2 G-****	2 Nov 09

800 kg discrepancy between required and uplifted fuel.

An aircraft was defueled for repairs to centre tank during a weekend shift of 3rd party contractor, at the end of which it needed refuelling. The Tech Log had been signed up for the repair work, but it did not show up the amount of fuel taken out to facilitate the repair nor the amount of uplift required to make up for the amount defueled. The Tech Log showed only the arrival fuel state from the previous sector. The aircraft was filled up to the required amount, but it needed 800 Kg more than the estimated amount calculated using the arrival fuel state as the baseline.

Comments: Clearly the 800 kg was the amount that had been taken out from the arrival fuel state to enable repair to take place. The error was that proper records were not placed on the Tech log for the amount of fuel taken out, and the amount of fuel either put back (or needed) to make up for the defueled amount. There were the elements of a system failure here with potentially serious consequence, if the situation got overlooked by other pressures and an aircraft got released with a smaller fuel load than what one assumed it to contain.

Serial No	Report No	Aircraft	Date
63	X398/**/**/****	Type_A2 G-****	13 Nov 09

Rumbling noise coming from nose wheel increasing with speed.

Aircraft was on ****** to ****** sector. Flight crew reported a rumbling noise coming from nose wheel, which increased as the speed increased.

The aircraft was inspected at ******** and it was found that the nose wheel retaining nut spacer was missing. The nut, nose wheel axle and sleeve were found undamaged.

A spacer was robbed from another company aircraft to repair this one, and then the aircraft was declared serviceable.

The mechanic who certified the last nose wheel change during "A" Check was interviewed, and reassured that he had completed the work exactly as per the AMM. He had no idea how the spacer came to be missing, and could offer “fretting fatigue” of the shim/spacer as one explanation.

Comments: There was no information on the date when the previous wheel change was done or the state of the condition of the spacer at that time. Therefore, there was no way of cross checking his explanation. If fretting was the main causal factor, then one would assume that the mechanic would have checked the state of the spacer and reported. Periodicity of A-Check is normally 14-day, so it might be possible that the checker had not noticed early signs of the spacer breaking up

Serial No	Report No	Aircraft	Date
64	X5/**/**/****	Type_A1 G-****	01 Jan 10

Aircraft slipped off axle jack during wheel change.

Engineers from the 3rd party contractors, **** *******, were maintaining the aircraft. At 04:30 AM, they were working outside on the aircraft parking bay under extremely severe weather conditions (-3 deg C, with ice and snow on the parking bay). The main wheel bogie was jacked up using a bottle jack to replace a worn No: 5 Main Wheel. The parking brakes had been released to enable the wheel retaining nut to be torque loaded. Concurrently aircraft was being unloaded.

Suddenly, the aircraft was jolted by a heavy container reaching the end of its travel, which made the aircraft to jump off the bottle jack.

On inspection it was found that the stone guard was cracked and the main wheel bogie paintwork got damaged. As a precautionary measure, the bogie area that rested on the bottle jack was examined using eddy current technique; no cracking damage was detected. A White ADD was entered to ensure that the cracked stone guard was replaced when a spare was available.

A MEDA investigation followed. It was revealed that changing the wheels under loading conditions had been an on-going accepted mode of operation. On this occasion the situation was compounded by the severe inclement weather and the need to release the aircraft stand ASAP. The team was working under time-pressure. Irrespective of that, the engineer had claimed that it was not possible to predict the occurrence of a sudden jolt by a heavy container.

However the investigator acknowledged that contractors need to take extra precautions during inclement weather, and a circular has been issued to draw attention the need for extra precautions.

An MOR has been sent to UK CAA.

Comments: Wheel changing with bottle jacks in position in concurrent with loading and unloading appears to be a set recipe for an accident. If this routine has been accepted as a standard mode of operation may be a moot point. Clearly this is an area of conflict between commercial policies (where rapid loading and unloading of revenue earning payloads is a critical factor) and safety policies. It might be possible that engineers were not exercising lateral thinking before bottle jacking aircraft when it is obvious that loading and unloading could sway the aircraft and extend or retract the shock absorbers, as cargo bay contents changed. Severe weather in this situation only aggravated the likelihood of an accident. Furthermore, releasing the brake in anticipation of torque loading was probably premature, that puts the aircraft at risk. A sloping bay could make the aircraft roll, and under icy conditions the situation could lead to a fatal accident. The closing action appeared to be glossing over the serious nature of this accident attributed to human error.

Serial No	Report No	Aircraft	Date
3	X32/**/**/****	Type_A3 G-****	15 Jan 10

APU bleed tube not connected after maintenance.

On 15 Jan 10, an engineer from a 3rd party contractor (******) on night shift was tasked to replace the APU Surge Valve Filter of a Type_A3 that was being prepared for a revenue flight to *******. Extreme cold weather conditions prevailed. In the middle of his, the engineer took a break by going into the warmer environment of the cockpit. On his return after the break, he overlooked the need to reconnect the APU bleed valve tube which he had previously disconnected as part of the AMM procedure. On completion of his somewhat "incomplete installation" he had conducted the required functional checks on the system, signed up for the work, certified for its integrity and released the aircraft to service.

During the subsequent handling and despatch phase, engines failed to start up on push back for which APU is used usually. Misidentifying the reasons for failure to start, the captain opted for a ground power assisted start; when the engineer arrived at the gate the engine was already running. This chain of event might have distracted the engineer from considering if his previous work had anything to do with the engine starting problem.

Eventually, there was a small technical delay, but the captain anxious to get away due to time pressures departed for *******.

After the aircraft departed, the engineer, realizing his mistake and its connection to the engine start up failure, reported making an error when wrapping up the task he handled.

The matter was passed on to ******. On inspecting the aircraft that arrived, investigators found that the bleed tube was indeed disconnected. This was reconnected and the system functionally tested and found satisfactory. The aircraft was released to service.

Investigations that followed had identified "distraction" as the primary cause of the omission leading to incomplete maintenance, and the time pressures and the involvement of ground power unit as contributory causes that eclipsed the error coming to the surface,

Considering the seriousness of potential consequences, actual damage was light. Only up to 30 – 60 min delay occurred at the departing station and thanks to information conveyed there was no delay at *****.

However it should be noted that the outward flight carried a fault that could have undermined ETOPS 180 clearance. Inability to start the engines in the event of a double flame out would have been disastrous.

Comments: The report does not offer recommendations to alleviate or prevent recurrence of such situations. Distraction of the individual due to extreme cold weather was the main causal factor, and time pressure as secondary factor that prevented a proper diagnosis for the failure to start engines.

Serial No	Report No	Aircraft	Date
16	X35/**/**/****	Type_A2 G-****	16 Jan 10

Smouldering fire in electrical wiring.

Thursday 14th January the aircraft was AOG in ********* due to a “FWD CABIN TEMP” EICAS message. The aircraft was released IAW MEL 21-61-1 and PADD 03/10 was raised. Saturday 16th January, the aircraft was on weekend maintenance and the engineers in ***** were tasked with investigating the "FWD CABIN TEMP" EICAS message. During the investigation, evidence of a fire was found in the mix manifold area. There were marks of a smouldering fire and burnt wires in wire bundles 4106 and 2447. Further investigation revealed metal chips inside a wire bundle.

Burnt wires in both bundles were repaired. Several burnt isolation blankets were removed and due to no spares being available WADD 01/10 was raised. The forward cabin trim air valve was found to be unserviceable and this was replaced IAW AMM.

An operational and system check of the primary temperature control system was carried out satisfactorily. A leak check of the forward cabin trim air duct and the right hand pack to mix manifold supply duct were carried out satisfactorily. A continuity check of wire bundles 4106 and 2447 was carried out satisfactorily.

It has been suggested that “the phenomenon of ageing aircraft be considered” in case fire was caused by loss of insulation that in turn could be attributed to hardness and brittleness of insulation material with age.

Comments: If aging wiring is the source of fire in this case, this event falls into the realm of “design and reliability” rather than human error. However if the issue concerns a failure to detect hardening insulation material in cables during the conversion process and associated structural and system survey, then human error at Part 21 (equivalent) Production Organization was possible.

Alternatively, if cable fraying due to metallic chips was the causal factor, then there should be an explanation for the origin or source of metallic chips. The report does not cover that point. One could speculate that they could be left-over residue from a previous structural repair (See similar incident, Case No: 13, 22 Jan 10, which described a burnt loom just below where structural repairs had been carried out).

Serial No	Report No	Aircraft	Date
15	X34/**/*/****	Type_B1 OO-****	19 Jan 10

Incomplete APU Bleed Valve Assembly fitted and incomplete installation.

On replacement of the APU bleed valve it was noticed that the valve fitted to the aircraft was incomplete in assembly. There should be two connectors fitted to the valve, one for the operating solenoid and one for the position indicating. There was only one connector fitted and this was to the solenoid.

On investigation in the AMM and IPC and checking the layout of the new replacement valve, it was found that the fitted valve had no switching unit or electrical receptacle fitted which is used for indicating the correct valve position in the cockpit. Further investigation revealed that the connector for the position indicator had been jammed behind the fire wire on the right hand wall of the APU bay with no protection.

A full assembly replacement was fitted and connector installed, functionally tested and the aircraft returned to serviceable state.

Comments: Clearly this is a case of an unsatisfactory spare infiltrating into the system, and the failure by the engineer who originally fitted the components to spot the faults. Detailed investigation of historical details has yet to be completed.

Serial No	Report No	Aircraft	Date
13	X21/**/**/****	Type_A2 G-****	22 Jan 10

Burnt and separated wiring in a loom.

On aircraft power up for departure, the RAT Pressure Light and the No.1 Engine Start Lights were both on indicating a fault. L ENG OVHT loop 2 & L ENG fire loop 2 EICAS status messages were displayed and the standby ignition 2L had tripped. During troubleshooting the No.1 Engine Start Valve and the APU Fuel Shut Off Valve CBs had tripped.

The fault was traced to a burnt loom which had caused 13 wires to short and then separate. The damaged loom was below the floor forward of the P50 card file on the right side of the aircraft. There was evidence of floor beam repair above the damaged loom.

The aircraft had undergone conversion at a Part 21 Production Organization in the US, where extensive structural repairs had been carried out.

Although there was no direct attribution, but it would suggest that the loom might have been either accidentally damaged during repairs to the floor beam, or if not loom damaged by corrosive substances coming from payloads carried in the past or cabin services that might have caused the floor beam to be corrode.

Comments: This incident could be attributed to human error but the origin is uncertain and further search might not be cost effective. It has remained as a dormant error, but the potential risk due to fire hazard should be taken as serious. Even if the original fault was due to corrosive fluid carried by a previous operator or from cabin services, it was the responsibility of the production organization tasked with the conversion to properly inspect and rectify corrosion defects or any other co-lateral damage to wiring. In this case, on the face of it, PO seemed to have failed in that responsibility

History of the aircraft, role, age, sectors flown and number of C-Check cycles may be relevant to this error finding. These parameters are included in the CAW Risk Model for future benefit.

Serial No	Report No	Aircraft	Date
17	X68/**/**/****	Type_A2 G-****	11 Feb 10

Insufficient bleeding of hydraulic system after leg replacement.

On arrival of the aircraft a daily inspection was carried out, during which it was found that the hydraulic contents were low on all three systems. EICAS contents were confirmed with reservoir sight-glass and replenishment point remote gauge. The hydraulics was replenished and leak checks of all systems were carried out. No leaks were evident, and full range functions of the flying controls were carried out several times and the contents remained stable. The maintenance history of the hydraulic system was reviewed and it was noted that the left main gear had been replaced at the previous station. Engineers had diagnosed that the hydraulic system had not been "bled" sufficiently after triple leg replacement prior to the last flight.
Investigation of the safety report is in progress. Causal factors would be determined in the course of this investigation.

Comments: No further comments as investigation has yet to be completed.

Proforma used for analyzing narrative error reports

Index	Node Name _ Secondary Level	Tertiary Level CF	State
1	**Operation and Capability**		
1.1	Aircraft Type and Series Fixed Wing		
1.2	Aircraft Type and Series Rotary Wing		
1.3	Registration Number		
1.4	Aircraft Age		
1.5	Number of Sectors Flown		
1.6	Number of Major Maintenance Cycles		
1.7	Aircraft		Combines error probability from nodes 1.1-1.6
1.8	Aircraft Generation Time		TR Time
1.9	Operating Role		
1.10	Route		
1.11	Nature of Operation		Combining error probability from nodes 1.8-1.10
1.12	Flight Origin		
1.13	Destination		
1.14	Departure Time		Intended for correlating shift hours and error.
1.15	Geographical Location & Time		Combining error probability from nodes 1.12-1.14
1.16	Fleet Size to Num Cat A Staff		
1.17	Fleet Size to Num Cat B1 Staff		
1.18	Fleet Size to Num Cat B2 Staff		
1.19	Fleet Size to Num Cat C Staff		
1.20	Fleet Size to Non Cat Tech Staff		
1.21	Technical Staff		Combining error probability from nodes 1.16-1.20
1.22	Fleet Size to Logistic Staff		
1.23	Fleet Size to Tech Managers		
1.24	Other Support Staff		Combining error probability from nodes 1.122-1.23
1.25	Staff Complement		Combining error probability from nodes 1.121-1.24
1.26	Operation V Capability		Combining error probability from nodes 1.7, 1.11, 1.15, 1.21, 1.24, 1.25

2	**Part 21 AO Regulation Compliance**		
2.1	Pt 21 Sub Part A General Provisions		
2.2	Pt 21 Sub Part J Design Organization Approval		
2.3	Pt 21 Sub Part G Production Organization Approval		
2.4	Pt 21 Sub Part F Production without POA		
2.5	Design and Production		Combining error probability from nodes 2.2-2.4
2.6	Pt 21 Sub Part B Type Certificates		
2.7	Pt 21 Sub Part D Changes to Type Certificate		
2.8	Pt 21 Sub Part E Supplemental Type Certificate		
2.9	Type Certificate		Combining error probability from nodes 2.6-2.8
2.10	Pt 21 Sub Part H Airworthiness Certificate		
2.11	Pt 21 Sub Part I Noise Certificate		
2.12	Certificates		Combining error probability from nodes 2.9-2.11
2.13	Pt 21 Sub Part K Parts and Appliances		
2.14	Pt 21 Sub Part M Repairs		
2.15	Pt 21 Sub Part O ETSO Authorization		
2.16	Pt 21 Sub Part Q Identification of Products		
2.17	ETSO		Combining error probability from nodes 2.15 - 2.16
2.18	Pt 21 Compliance		Combining error probability from nodes 2.5, 2.9, 2.12, 2.14, 2.15, 2.17
3	**Part M AO and Pt 145 AO Regulation Compliance**		
3.1	Part 145 AO Findings Level 1		
3.2	Part 145 AO Findings Level 2		
3.3	Compliance 145		Combining error probability from nodes 3.1 – 3.2
3.4	Pt M Sub Pt B Findings Level 1		
3.5	Pt M Sub Pt B Findings Level 2		
3.6	Pt M Sub Pt B Compliance		Combining error probability from nodes 3.4 – 3.5
3.7	Pt M Sub Pt C Findings Level 1		

3.8	Pt M Sub Pt C Findings Level 2		
3.9	Pt M Sub Pt C Compliance		Combining error probability from nodes 3.7 – 3.8
3.10	Pt M Sub Pt D Findings Level 1		
3.11	Pt M Sub Pt D Findings Level 2		
3.12	Pt M Sub Pt D Compliance		Combining error probability from nodes 3.10 – 3.11
3.13.	Pt M Sub Pt E Findings Level 1		
3.14	Pt M Sub Pt E Findings Level 2		
3.15	Pt M Sub Pt E Compliance		Combining error probability from nodes 3.13 – 3.14
3.16	Pt M Sub Pt G Findings Level 1		
3.17	Pt M Sub Pt G Findings Level 2		
3.18	Pt M Sub Pt G Compliance		Combining error probability from nodes 3.16 – 3.17
3.19	Pt M Sub Pt H Findings Level 1		
3.20	Pt M Sub Pt H Findings Level 2		
3.21	Pt M Sub Pt H Compliance		Combining error probability from nodes 3.19 – 3.20
3.22	Pt M Sub Pt I Findings Level 1		
3.23	Pt M Sub Pt I Findings Level 2		
3.24	Pt M Sub Pt I Compliance		Combining error probability from nodes 3.22 – 3.23
3.25	Compliance M		Combining error probability from nodes 3.6, 3.9, 3.12, 3.15, 3.18, 3.21, 3.24
3.26	Pt 145 and Pt M Compliance		Combining error probability from nodes 3.3, 3.25, 9.12
4	**Pt 21 AO Error Performance (Active or Dormant)**		
4.1	Aircraft Design		
4.2	Reliability and Maintainability Tests		
4.3	Production		
4.4	Product		Combining error probability from nodes 4.1 – 4.3
4.5	Maintenance Manuals		
4.6	Product Training		
4.7	OEM Spares		
4.8	Pt 21 AO Product Support		Combining error probability from nodes 4.5 – 4.7

4.9	Pt 21 AO / Pt M AO Product Support Contract		
4.10	Pt 21 and Pt M Interface		Combining error probability from nodes 4.8 – 4.9
5	**Pt M AO Error Performance (Active or Dormant)**		
5.1	Pt M Sub Pt B Accountability		
5.2	Pt M Sub Pt C Continuing Airworthiness		
5.3	Pt M Sub Pt D Maintenance Standards		
5.4	Pt M Sub Pt E Components		
5.5	Pt M Sub Pt G CAMO		
5.6	Pt M Sub Pt H CRS		
5.7	Pt M Sub Pt I Airworthiness Review		
5.8	Pt M Organization		Combining error probability from nodes 5.1 – 5.7, 9.12
5.9	Pt M and Pt 145 Contract Interface		
5.10	Pt M and Pt 145 Interface		Combining error probability from nodes 5.8 – 5.9
6	**Pt 145 AO Error Performance (Active or Dormant)**		
6.1	Pt 145 Organizational Performance		Combining error probability from nodes 5.10, 9.12
6.2	Maintenance Data		
6.3	Ground Support Equipment		
6.4	Tools and Test Equipment		
6.5	Line Replacement Units and Spares		
6.6	Facility and Environment		
6.7	Logistic Support		Combining error probability from nodes 6.2 – 6.6
6.8	Task Management Documents		
6.9	Manning		
6.10	Attitude to Task		Combining error probability from nodes 6.8 and 6.11
6.11	Workface Stress		Combining error probability from nodes 6.9, 7.12
6.12	Task		Combining error probability from nodes 6.7, 6.8, 6.11
6.13	Pt 145 Performance		Combining error probability from nodes 5.9, 6.12

7	**Individual Factors (Active or Dormant)**		
7.1	Training and Qualification		
7.2	Health and Fitness		
7.3	Pt 66 Licensing		Combining error probability from nodes 7.1, 7.2
7.4	Competence		
7.5	Continuation Training		
7.6	Technical Knowledge and Skills		Combining error probability from nodes 7.4, 7.5
7.7	Certification and Recertification		
7.8	Physiological Limits		
7.9	Physical Health		
7.10	Personal Stress		
7.11	Health and Welfare		Combining error probability from nodes 7.9, 7.10
7.12	Individual Traits		Combining error probability from nodes 7.7, 7.8, 7.11
8	**QMS Organization and Performance**		
8.1	CAW Quality Policy		
8.2	Quality Plan and Programs		
8.3	Quality Audit Scope		
8.4	Resources and Training Standards		
8.5	Audit Procedure		
8.6	Remedial Action Procedure		
8.7	CAW Management Activity		
8.8	Monitor Effectiveness of Aircraft Maintenance Program		
8.9	Maintenance Contract Monitoring		
8.10	QMS Policy and Plans Scope		Combining error probability from nodes 8.1-8.4
8.11	QMS Tasks and Processes		Combining error probability from nodes 8.5 – 8.9
8.12	QMS Organization		Combining error probability from nodes 8.10, 8.11
8.13	Pt M Management Activity		
8.14	Pt M Finding Reporting		
8.15	Pt M Corrective Action		

8.16	Pt M Quality Audit Performance		Combining error probability from nodes 8.13 – 8.15
8.17	Pt 145 Activity Area		
8.18	Pt 145 Finding Reporting		
8.19	Pt 145 Corrective Action		
8.20	Pt 145 Quality Audit Performance		Combining error probability from nodes 8.17 – 8.19
8.21	Sub Contractor Activity Area		
8.22	Sub Contractor Finding Reporting		
8.23	Sub Contractor Corrective Action		
8.24	Sub Contractor Quality Audit Performance		Combining error probability from nodes 8.21 – 8.23
8.25	Supplier Activity Area		
8.26	Supplier Finding Reporting		
8.27	Supplier Corrective Action		
8.28	Supplier Quality Audit Performance		Combining error probability from nodes 8.25 – 8.27
8.29	Quality Audit Performance		Combining error probability from nodes 8.16, 8.20, 8.24, 8.28
8.30	Quality Management System		Combining error probability from nodes 8.12, 8.29, 10.6
9	**Corporate Policy and Global Factors**		
9.1	Global factors		
9.2	Central Government		
9.3	Local Government		
9.4	Corporate Board		
9.5	Trade Union		
9.6	CEO AM Decisions		Combining error probability from nodes 9.1 – 9.5
9.7	Commercial Policies		
9.8	Flight Operations Policies		
9.9	Engineering Operations Policies		
9.10	Logistic Support Policies		
9.11	Human Resources Policies		
9.12	Corporate and Policy Issues		Combining error probability from nodes 9.7 – 9.11, 10.6

10	**Change Management**		
10.1	Business Management		
10.2	Flight Operations		
10.3	Maintenance Organization Exposure		
10.4	Engineering and Technology		
10.5	Human Resources		
10.6	Change Management		Combining error probability from nodes 10.1 – 10.5, 9.6
11	**Error Probability Defences and Consequences**		
11.1	CAW Management		Combining error probability from nodes 4.4, 5.8, 6.13, 11.2
11.2	Defence Pt 145		
11.3	Consequences Pt 145		
11.4	Release to Fly		Combining error probability from nodes 11.1, 11.5
11.5	Defence Pt M		
11.6	Consequences Pt M		
11.7	Handling and Despatch		Combining error probability from nodes 3.26, 8.30, 9.12, 11.4, 11.8,
11.8	Defence H and D		
11.9	Consequence H and D		
11.10	Defence Pre Take Off		
11.11	Take Off		Combining error probability from nodes 11.7, 11.10
11.12	Consequence Pre Take Off		
11.13	Flight and Consequences		
11.14	Combined Cost		Combining error probability from nodes 11.3, 11.6, 11.9, 11.13, 11.14, 11.5, 11.6
11.15	Defence Quality		Late additions for validation
11.16	Consequence Quality		Late additions for validation